Inspector General
United States
Department *of* Defense

Accountability for Defense Security Service Assets
With Personally Identifiable Information

			Form Approved
Report Documentation Page			OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **24 JUL 2008**	2. REPORT TYPE	3. DATES COVERED **00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Accountability for Defense Security Service Assets With Personally Identifiable Information	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense Inspector General,ODIG-AUD,400 Army Navy Drive,Arlington,VA,22202-4704**	8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**66**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Acronyms

ASD(NII)/CIO	Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer
CAC	Common Access Card
DMDC	Defense Manpower Data Center
DPAS	Defense Property Accountability System
DRMO	Defense Reutilization and Marketing Office
DSS	Defense Security Service
IG	Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSD	Office of the Secretary of Defense
PII	Personally Identifiable Information
PSI	Personnel Security Investigation
US-CERT	U.S. Computer Emergency Readiness Team
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics

July 24, 2008

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION,
TECHNOLOGY, AND LOGISTICS
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
DIRECTOR OF ADMINISTRATION AND MANAGEMENT
DIRECTOR, DEFENSE SECURITY SERVICE

SUBJECT: Report on Accountability for Defense Security Service Assets With Personally
Identifiable Information (Report No. D-2008-114)

We are providing this report for review and comment. We considered management
comments on a draft of this report in preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. We
request that the Under Secretary of Defense for Acquisition, Technology, and Logistics provide
additional comments on Recommendation 2.b. As a result of management comments, we revised
Recommendation 3. to clarify our intention. We request that the Director of Administration and
Management provide additional comments on revised Recommendation 3. In addition, based on
events that occurred after the issuance of the draft report, we removed Recommendations 1.f., 1.g.,
1.h., and 1.i. and renumbered the other parts of Recommendation 1. accordingly. Management
should provide comments on the final report by August 25, 2008.

If possible, please send management comments in electronic format (Adobe Acrobat file
only) to AUDROS@dodig.mil. Copies of the management comments must contain the actual
signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual
signature. If you arrange to send classified comments electronically, they must be sent over the
SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff as well as the excellent assistance
provided by the DSS staff. Questions should be directed to Ms. Rhonda L. Ragsdale at (703)
604-9347 (DSN 664-9347) or to Mr. Robert P. Goldberg at (703) 604-9218 (DSN 664-9218). See
Appendix E for the report distribution. The team members are listed inside the back cover.

Paul J. Granetto
Principal Assistant Inspector General
for Auditing

Report No. D-2008-114   **July 24, 2008**

(Project No. D2007-D000LC-0042.000)

Accountability for Defense Security Service Assets With Personally Identifiable Information

Executive Summary

Who Should Read This Report and Why? The management at the Defense Security Service (DSS) and personnel concerned with property accountability should read this report because it discusses accountability for assets that contain personally identifiable information (PII) and the requirements for reporting unauthorized disclosure of PII.

Background. DSS provides the Secretary of Defense, DoD Components, and Defense contractors security support services. In February 2005, DSS transferred responsibility for the personnel security investigation function to the Office of Personnel Management (OPM), along with 1,567 DSS employees. The former Director of DSS also transferred common access cards (CACs), safes, laptops, and auxiliary hard drives to OPM.

Results. DSS management in place during the transfer of the personnel security investigation function to OPM created a lack of accountability for assets, posing an undue risk of compromising PII for military, civilian, and contractor employees who were investigated for personnel security clearances between 1997 and 2005. Through substantial efforts of its current management, DSS located and confirmed by unique identifier 308 of an estimated 501 initially unaccounted-for laptops. DSS obtained additional information demonstrating reasonable assurance that the remaining 193 laptops did not leave control of Government personnel; therefore, PII contained on the laptops is not at risk. Although DSS has accounted for the 501 initially unaccounted-for laptops, the initial listing of 501 laptops was not accurate. Additional laptops may still need to be accounted for.

DSS demonstrated to the Defense Privacy Office that there was no indication the unaccounted-for laptops had left the control of Government personnel. Based on the information provided by Defense Security Service, the Defense Privacy Office concluded that the risk of unauthorized disclosure of PII was not high enough to warrant public notification. Consequently, DSS did not issue a public notification. Although the Defense Privacy Office determined no public notification was warranted, a risk of unauthorized disclosure of PII still exists if laptops still remain unaccounted-for. To prevent recurrence of a lack of accountability for assets, the Director of the Defense Security Service should implement controls over property that contains sensitive or classified information or PII, conduct periodic physical inventories of assets that contain PII, and track assets containing PII by unique identifier.

Although the current DSS management inherited inaccurate property records, it is responsible for correcting them. A review of 50 DSS property records showing custody of electronic devices such as laptops showed only 23 of 50 property records were accurate. DSS internal controls were not adequate. We identified material weaknesses in property

accountability for DSS assets. Current DSS management is aware of the weaknesses and has developed an action plan with objectives for FY 2008.

Management Comments and Audit Response. The Director of Acquisition Resources and Analysis in the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]) provided comments. She concurred with revising DoD Instruction 5000.64 to state that the policy applies to mobile computing devices including but not limited to laptops, mobile information storage devices, and auxiliary hard drives, regardless of dollar threshold. She partially concurred with requiring that all DoD Components include unique identifiers on Defense Reutilization and Marketing Office (DRMO) turn-in documents when disposing of laptops and other electronic devices that may contain PII. The Director stated guidance in two memoranda not cited in the report may eliminate the need for the recommendation. The memoranda are:

- Deputy Secretary of Defense Directive Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," May 29, 2001; and

- Assistant Secretary of Defense for Command, Control and Communications Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001.

While we considered the response to the recommendation to update DoD Instruction 5000.64 responsive, we ask the Director to reconsider her position on the recommendation regarding unique identifiers on DRMO turn-in documents and provide comments by August 25, 2008. The suggested guidance does not address accountability for laptops as they are turned in to the DRMO for disposal.

The DoD Senior Agency Official for Privacy did not concur with our recommendation to continue working with the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer and the USD(AT&L) to develop overarching guidance on the protection of PII on mobile computing devices. The Senior Agency Official stated that overarching guidance would create confusion. We clarified the recommendation. Its intent was to create one memorandum that would direct DoD officials to the proper guidance on protecting PII, accounting for assets that are sensitive, and reporting a potential breach of PII. We request that the Senior Agency Official for Privacy comment on the revised recommendation by August 25, 2008.

The DSS Director concurred with six of the recommendations and nonconcurred with four. The Director determined that the two recommendations related to unaccounted-for laptops—to continue coordinating with OPM to locate additional laptops, and to plan and mitigate the risk of unauthorized disclosure of PII—were no longer necessary because DSS has resolved the last 7 of the 501 initially unaccounted-for laptops. We agree DSS has demonstrated reasonable assurance that the 501 initially unaccounted-for laptops have been accounted for. Therefore, we removed the recommendations to continue to work with OPM to resolve remaining unaccounted-for laptops and implement steps to mitigate risk of unauthorized disclosure of PII. However, because 501 was not an accurate baseline, additional laptops may still need to be accounted for. The Director also determined that the remaining seven unaccounted-for CACs were issued to former DSS employees after they transferred to OPM and were not the responsibility of DSS. We agree that the remaining seven unaccounted-for CACs are not the responsibility of DSS and removed the recommendation on CACs. The Director determined that through due diligence DSS has mitigated the risk of any possible unaccounted-for safes. We agree and removed the recommendation on safes. See the Finding section for a discussion of management comments and the Management Comments section for complete text of the comments.

Table of Contents

Background

Defense Security Service Mission and Functions. The Defense Security Service (DSS) provides the Secretary of Defense, the DoD Components, Federal Government contractors, and 23 other Federal agencies with a full range of security support services. These services include security education, security training, and technical services involved in the industrial security clearance process. Prior to February 2005, DSS also performed personnel security investigations (PSIs) for these organizations. DSS reports to the Under Secretary of Defense for Intelligence. DSS is headquartered in Alexandria, Virginia, and has field offices throughout the United States. Within DSS the person responsible for property accountability is the Director, who has delegated this responsibility to the property book officer.

Transfer of Functions From DSS to the Office of Personnel Management. In FY 2003, the Deputy Secretary of Defense and the Director, Office of Personnel Management (OPM) agreed to transfer responsibility for the PSI function from DSS to OPM. DoD made this transfer to improve the timeliness of investigations, recognizing the success that OPM and the private sector achieved in that area over the last several years. The transfer was accomplished through two memoranda. The first memorandum of understanding, dated January 24, 2003, expressed the intent of DoD and OPM to obtain statutory authority to transfer the PSI function from DoD to OPM. The second memorandum of agreement, "Transfer of Certain Elements of the U.S. Department of Defense to the U.S. Office of Personnel Management," October 16, 2004, identified the number of personnel to transfer and detailed the costs of the transfer as well as the responsibility for the personnel being transferred. Specifically, it stated that approximately 1,800 employees who performed work related to the PSI function would transfer to OPM. The memorandum also set the goal for OPM to manage the PSI function by February 20, 2005. OPM requested DoD to provide support services on a reimbursable basis for payroll, facilities, and information technology.

Assets Transferred. In February 2005, DSS transferred 1,567[1] PSI-related positions and $33.8 million to OPM. In addition, DSS transferred common access cards (CACs),[2] approximately 1,483 laptops, and an undetermined number of safes and auxiliary hard drives. As part of the transfer, OPM took over the responsibility for some of the former DSS field offices located throughout the United States that performed PSIs.

Transfer Responsibilities. DoD established a 15-member transition team to coordinate the PSI transfer to OPM. The team was charged with ensuring the transfer occurred by February 2005 in accordance with the timelines established in the October 16, 2004, memorandum of agreement. The Under Secretary of Defense for Intelligence approved the transition team members, including the Deputy Under Secretary of Defense for Counterintelligence and Security, the Acting DSS Director, the DSS Deputy Director of Personnel Security, and the DSS Deputy Director of Industrial Security.

---

[1] The October 16, 2004, memorandum estimated that 1,800 employees would transfer to OPM; however, in February 2005, only 1,567 employees actually transferred to OPM.

[2] The CAC is used as a general identification card as well as for authentication to gain access to DoD computers, networks, and certain DoD facilities.

According to the Deputy Associate Director of OPM, the transition team and OPM management entered into an informal, verbal agreement regarding the transfer of assets. Specifically, they agreed that PSI investigators could take DSS laptops and CACs with them to OPM to complete ongoing investigations. The intent was that the investigators would return the laptops as well as their CACs to DSS when the ongoing investigations were completed. In addition, DSS agreed to purchase auxiliary hard drives for the transferring investigators to access OPM's automated system until they completely transitioned to PSI cases originating through OPM. The informal, verbal agreement also allowed OPM to take possession of an undetermined number of safes.

Guidance on Security of Personally Identifiable Information. Personally Identifiable Information (PII) is defined in Office of Management and Budget (OMB) memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," July 12, 2006, as any information that can be used to trace an individual's identity. Since 2002, both DoD and OMB have issued policies on accountability for and security of PII.

DoD Guidance on Accountability for Property. DoD Instruction 5000.64, "Defense Property Accountability," August 13, 2002, requires DoD Components to keep accountable property records and transaction trails for all property that has an acquisition cost greater than $5,000 or constitutes sensitive[3] or classified assets. The guidance also discusses accountability requirements for assets lent to non-DoD agencies and accountability for pilferable items (such as laptops). Specifically, it states that DoD Components shall establish records and maintain accountability for property furnished to such agencies or contractors.

DoD Instruction 5000.64, "Accountability and Management of DoD-Owned Equipment and Other Accountable Property," November 2, 2006, replaced the 2002 version and allows DoD Components to assess the vulnerability of pilferable property and determine how they will account for it. However, the revised instruction, like the 2002 version, maintains that accountable property records should be established for assets that are sensitive or classified and for assets that are transferred to other Government agencies.

Defense Property Accountability System. The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]) requires that DoD Components use a fully operational property accountability system that meets Federal accounting standards and can capture and maintain historical data. Further, the Under Secretary of Defense (Comptroller)/ Chief Financial Officer designated the Defense Property Accountability System (DPAS) as the property system for DoD.

Office of Management and Budget Reporting Requirements. OMB memorandum, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments,"

---

[3] According to the Director of Administration and Management, Department of Defense Senior Privacy Official Memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," September 21, 2007, PII is information about an individual that identifies, links, relates, or is unique to or describes him or her. Examples of PII include but are not limited to Social Security number; age; military rank; civilian grade; marital status; race; salary; home/office phone number; and other demographic, biometric, personnel, and medical information. Although PII does not meet the strict definition of sensitive information in DoD Instruction 5000.64, the Director of the Defense Privacy Office considers PII sensitive information.

July 12, 2006, requires that agencies report all incidents involving PII to the U.S.Computer Emergency Readiness Team (US-CERT), an organization within the Department of Homeland Security, within 1 hour of discovering them. Specifically, the July 12, 2006, memorandum states:

> This memorandum revises those reporting procedures to now require agencies to report all incidents involving personally identifiable information to US-CERT within one hour of discovering the incident. You should report all incidents involving personally identifiable information in electronic or physical form and should not distinguish between suspected and confirmed breaches. US-CERT will forward all agency reports to the appropriate Identity Theft Task Force point-of-contact also within one hour of notification by an agency.

OMB requires prompt reporting to US-CERT so US-CERT can assess the potential impact on national security and quickly notify the proper authorities of breaches that could affect national security. DoD Directive 5400.11-R, "DoD Privacy Program," May 14, 2007, defines a breach as the actual or possible loss of control, or unauthorized disclosure of or access to personal information such as Social Security number, a person's medical history, financial information, or criminal information. The memorandum further states that an agency should report all breaches regardless of whether they are suspected or confirmed. However, under US-CERT reporting requirements, while an incident is under investigation to determine whether information was compromised, the 1-hour reporting requirement is not applicable. According to a US-CERT Official, when the investigation is complete, the agency should report the results of the investigation to US-CERT. Once it receives a report of a breach, US-CERT forwards the report to the Identity Theft Task Force, headed by the Attorney General at the Department of Justice within 1 hour of the agency notifying US-CERT. President Bush established the Identity Theft Task Force to strengthen and improve the Government's ability to improve the Nation's awareness, prevention, detection, and prosecution of identity theft.

Office of the Secretary of Defense Guidance. The Director of the Defense Privacy Office reports to the DoD Director of Administration and Management in the Office of the Secretary of Defense (OSD). The Defense Privacy Office has responsibility for developing policy, providing program oversight, and serving as the DoD focal point for DoD privacy matters. The DoD Director of Administration and Management, who serves as the Senior Privacy Official for DoD, issued a memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," September 21, 2007, which implements the OMB requirements for reporting breaches to US-CERT. The memorandum states that, in addition to reporting to US-CERT, DoD Components must report both confirmed and unconfirmed breaches of PII to the Defense Privacy Office within 48 hours of becoming aware of them. The Defense Privacy Office requires prompt reporting so it can react quickly to breaches that have high potential for causing harm, such as identity theft, to affected individuals.

The memorandum also requires the DoD Component that identifies the incident to determine the level of risk of harm, such as identity theft or the disclosure of embarrassing information that could affect one's reputation. Specifically, when a DoD Component determines whether notifying the general public is necessary, the Component should consider the likely harm and the likelihood of risk occurring. When assessing risk, the DoD Component should consider the following five factors:

- the nature of the data elements breached,

- the number of individuals affected,

- the likelihood that the information is accessible and usable,

- the likelihood that the breach may lead to harm, and

- the ability of the agency to mitigate the risk of harm.

The memorandum also urges agencies to "bear in mind that notification of a breach when there is little or no risk of harm might create unnecessary concern and confusion." The memorandum further states that the DoD Component will document its assessment of the level of risk and its rationale for not notifying the public.

Objectives

The objective of the audit was to determine whether DSS has adequate controls and accountability to secure its assets that contain sensitive personal data including CACs, safes, laptops, and hard drives. Specifically, we determined whether DSS properly secured assets as part of the transition of the PSI function from DSS to OPM. In addition, we reviewed the security of assets currently in the possession of DSS. See Appendix A for a discussion of the scope and methodology and Appendix B for prior audit coverage.

Review of Internal Controls

We identified material internal control weaknesses for DSS property accountability as defined by DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," January 4, 2006. Former DSS management deviated from DoD Instruction 5000.64 (both 2002 and updated 2006 versions) by not keeping a transaction trail for an estimated 501 laptops and an undetermined number of safes and auxiliary hard drives during the transfer of the PSI function from DSS to OPM. In addition, DSS deviated from DSS internal guidance when it allowed 48 DSS employees to leave DSS without collecting, deactivating, and disposing of their CACs. Although DSS has taken steps to improve its property accountability system, the audit team's review of a sample of property accounting records of electronic data devices from May to August 2007 indicated that only 23 of 50 property accounting records sampled were accurate.[4] Implementing Recommendations 1.a.-1.c. and 1.f. will improve property accountability at DSS. DSS identified property accountability as a weakness needing correction in its "Memorandum For the Secretary of Defense FY 2007 Annual Statement Required under the Federal Managers' Financial Integrity Act of 1982," August 20, 2007. To correct the inventory control weaknesses, current DSS management has established these planned objectives for FY 2008.

- Finalize and implement DSS policy and procedures for all categories of plant, property, and equipment.

- Complete an inventory of DoD property held by OPM and update DPAS.

- Complete an inventory of all items classified as sensitive property, and ensure items are properly accounted for in DPAS in accordance with DSS policy.

- Certify the inventory of sensitive property in DPAS.

- Verify that supporting documentation for reviews and inventories is generated and maintained in accordance with policy.

We will provide a copy of the report to the DSS office responsible for internal controls.

---

[4] The inventory reviews performed by the DoD IG audit team were limited to headquarters and field offices located in Linthicum, Maryland.

Accounting for Assets With Personally Identifiable Information

Through substantial efforts by current DSS management, the DoD Inspector General (IG) audit team, and OPM management to locate unaccounted-for assets, as of February 11, 2008, 308 out of an estimated 501 unaccounted-for laptops were recovered and confirmed by unique identifier. DSS obtained additional information demonstrating reasonable assurance that 186 of the remaining 193 did not leave control of Government personnel; therefore PII contained on the laptops is not at risk. DSS continued efforts to locate the seven remaining laptops.

A review of current DSS DPAS inventory records of information technology devices showed that, of a sample of 50 records reviewed, only 23 were accurate. DSS has recognized it has inaccurate inventory records and has documented corrective actions to be achieved in FY 2008.

In addition, as of December 13, 2007, DSS could not fully account for seven CACs and an undetermined number of safes.[5]

This inability to locate property occurred because DSS management at the time of the transfer of the PSI function from DSS to OPM did not:

- plan for the transfer from DSS to OPM of assets related to the PSI function,

- define property accountability requirements or oversee the contractor hired to collect and return DSS laptops lent to OPM, or

- maintain accurate property accountability records for safes, laptops, and auxiliary hard drives during the transfer of the PSI function to OPM in accordance with DoD Instruction 5000.64.

Current DSS management has not fully implemented planned improvements to property accountability.

As a result, DSS management in place during the transfer created a lack of accountability for assets, posing an undue risk of compromising PII for military, civilian, and contractor employees who were investigated for personnel security clearances between 1997 and 2005. However, because DSS has demonstrated to the Defense Privacy Office that there is no indication that the unaccounted-for laptops have left Government control and the Defense Privacy Office has concluded that the risk of unauthorized disclosure of PII on unaccounted-for laptops was not high enough to warrant public notification of compromised PII, DSS did not issue a public notification. Although the Defense Privacy Office determined no public notification is warranted, a risk of unauthorized disclosure of PII still exists for the seven remaining unaccounted-for laptops.

---

[5] In February 2008 DSS determined that OPM issued 7 of the 55 CACs to former DSS employees after they transferred to OPM.

Accountable Defense Security Service Property

The transfer of the PSI function from DSS to OPM included 1,567 people and approximately 1,483 laptops.[6] During the transfer, DSS also purchased an undetermined number of auxiliary hard drives for transferring DSS investigators. The hard drives allowed the investigators to access documentation stored on OPM's automated system for PSI investigations. In addition, DSS allowed 55 investigators to retain their CACs after transferring to OPM to facilitate their continued access to DoD facilities to complete ongoing investigations. DSS also allowed OPM to keep an undetermined number of safes used by DSS investigators to hold sensitive and classified information. According to the former Acting DSS Director, the transfer of assets was based on verbal agreements between the Special Assistant to the former Acting DSS Director and the OPM Director.

Laptops

Laptops Loaned to OPM. According to the former Assistant to the former Acting DSS Director[7] and the Deputy Associate Director of OPM, the verbal agreement between DSS and OPM included the loan of approximately 1,483 DSS laptops (valued at up to $2.2 million)[8] to OPM so that former DSS PSI investigators could complete ongoing investigations after transferring to OPM. According to the former Acting DSS Director, the verbal agreement was that OPM would return the laptops 6 months after the transfer.[9] However, OPM did not return all the laptops within 6 months. In fact, DSS continued to receive more borrowed laptops a year after the 6-month agreement had expired. Regardless of when they were returned, as DSS personnel received the laptops from OPM, they did not always update their property accountability records.

At the time of the transfer, DPAS records indicated that DSS had an inventory of approximately 2,826 laptops. According to DSS e-mail correspondence between the former Acting Director's Special Assistant and an official at the OSD Comptroller, DSS transferred 1,483 of the 2,826 laptops to OPM and instructed OPM to return them 6 months after the transfer (the remaining 1,343 were laptops retained for DSS use).

In December 2006 the Chief of DSS Support Services[10] had his staff perform queries of DPAS records and concluded that DSS could not account for 501 of the 2,826 laptops listed in DPAS. The audit team reviewed analysis performed by DSS staff of non-DPAS inventory records and found that DSS transferred 249 of the 501 unaccounted-for laptops to OPM and retained 252 for DSS operations. During the course of the audit, the DoD IG audit team, DSS, and OPM personnel located 308 of the 501 unaccounted-for laptops confirmed by unique identifier, leaving 193 other than physically accounted for. Table 1 displays the DSS laptop inventory prior to the transfer and summarizes the

---

[6] Although 1,567 DSS employees transferred from DSS to OPM, not all DSS employees took DSS laptops with them.

[7] The Acting Director during the transfer served from 2004 to 2005.

[8] This calculation assumes an average cost of $1,500 per laptop.

[9] The agreement for OPM to return the laptops to DSS was extended at least three times, until April 1, 2006.

[10] The Chief of Support Services is no longer employed at DSS.

unaccounted-for laptops from the start of the audit in December 2006 through February 11, 2008.

Table 1. DSS Laptop Inventory

	Related to PSI Transfer	Unrelated to PSI Transfer	Total DSS Laptop Inventory
	1,483	1,343	**2,826***
Unaccounted for		**501**	

	Related to PSI Transfer	Unrelated to PSI Transfer	Total
	249	252	**501**
Physically accounted for	133	175	**308**
Other than physically accounted for	116	77	**193**

*The 2,826 laptops are an estimate based on queries of DSS DPAS records of laptops that DSS used during the transition period. Since DPAS records were not accurate, we cannot be certain that the 2,826 laptops are not understated or overstated.

Although 116 of the 193 of the outstanding laptops were related to the transfer of the PSI function from DSS to OPM, 77 of the 193 unaccounted-for laptops were not related to the transfer of assets to OPM. The lack of accountability for laptops at DSS therefore is not solely a result of DSS transferring laptops to OPM, but also a result of DSS management not maintaining accurate records of their own laptops.

During the course of the audit, the DoD IG audit team, DSS, and OPM personnel located 308 of the 501 unaccounted-for laptops through the following steps.

- Between August 2006 and May 2007, DSS sent e-mails to all DSS employees requesting that they identify any laptops in their custody by unique identifier (serial number or bar code).

- Between March and June 2007, DoD IG and DSS staff searched nine DSS field offices.

- Between May and July 2007, DoD IG and OPM IG staff searched six OPM field offices.

- Between January 2007 and May 2008, DoD IG and DSS staff reviewed Defense Reutilization and Marketing Office (DRMO) and Directorate of Logistics documentation[11] to identify any laptops sent to DRMO offices for disposal or destruction.

- Between December 2006 and July 2007, DoD IG and OPM IG staff conducted interviews with former DSS and OPM property managers as well as former and current DSS and OPM employees listed in DPAS as the last to have custody of the unaccounted-for laptops.

- In August 2007, DSS convened a task force in response to the Deputy Secretary of Defense instruction to DSS to dedicate the resources necessary to locate the remaining unaccounted-for laptops.

Thanks to the joint efforts, as of February 11, 2008, 308 of the 501 laptops had been located and confirmed by a unique identifier, reducing the laptops DSS could not physically account for to 193. Table 2 shows the 308 laptops located and confirmed by unique identifier.

Table 2. Laptops Located as of February 11, 2008	
Laptops located at DSS headquarters	92
Laptops located at DSS field offices	91
Laptops located at OPM field offices	49
Laptops located at DRMO sites	62
Laptops located at commercial storage facility	14
Physically accounted-for laptops	**308**
Other than physically accounted-for laptops	**186**
Laptops remaining to be accounted for	**7**
Total	**501**

Through the efforts of a DSS dedicated task force, DSS obtained information that indicates 186 of the 193 laptops did not leave Government control. Therefore, PII on those laptops may not be at risk of unauthorized disclosure. Specifically, DSS has obtained the following information.

---

[11] The DRMO documentation reviewed included DD Forms 1348-1A, which DoD requires for turn-in of assets to the DRMO.

- DSS identified transaction trails in DPAS records that indicated 21 of the 193 laptops were incorrect entries in DPAS. The laptops were actually disposed of at the DRMO.

- DSS located DRMO turn-in documents that did not list unique identifiers such as serial numbers or barcodes but identified 65 laptops that DSS had disposed of at DRMO locations where DSS field offices had closed. According to DPAS records, DSS did not remove any laptops from the property books during these time frames, indicating that the 65 laptops are part of the 193 unaccounted-for laptops.

- DSS found DPAS records that showed that 55 of the remaining 193 laptops may not have been used for PSIs and therefore may not have PII on them.

- DSS certified that 3 of the 193 unaccounted-for laptops were replaced under warranty, but their records were not updated in DPAS.

- DSS located 42 hard drives from DSS and OPM field offices and matched them with 42 of the 193 unaccounted-for laptops by linking employee names contained on the hard drives to the employees that DPAS records showed were assigned to the laptops.

- DSS also identified 4,369 hard drives that DSS and OPM disposed of through the National Security Agency. However, because DSS disposed of these hard drives and there were no records by unique identifier, DSS cannot clearly determine whether any of them were part of the 501 unaccounted-for laptops. In addition, DSS located 1,292 hard drives that DSS personnel are currently analyzing; these hard drives will bring the total to 5,663. DSS plans to dispose of the hard drives after completing the analysis.

Table 3 shows the information provided by DSS regarding the remaining unaccounted-for laptops.

Table 3. Summary of Remaining Laptops as of February 11, 2008		
Unaccounted-for laptops		501
Located by unique identifier		308
Laptops not fully accounted for		193
Laptops accounted for by other than unique identifier		
Double counted in DPAS records	21	
Turned in to the DRMO without record of unique identifiers	65	
DPAS records show not used for PSIs	55	
Replaced under warranty	3	
Accounted for by hard drive	42	
Subtotal		186
Total unresolved laptops that may contain PII		**7**

In May 2008 DSS was able to resolve the remaining seven unaccounted-for laptops. DSS determined that personnel keying serial numbers into DPAS made a typographical error for each of the seven laptops. DSS compared DRMO turn-in documents and Directorate of Logistics[12] turn-in documents with the laptop records in DPAS and found that serial numbers for the seven laptops did not match the unique identifiers in DPAS records but were only one digit off. As a result, laptops located and confirmed by unique identifier as of May 2008 totaled 308; 193 were accounted for by other means. According to DSS, the information presented demonstrates the previously unaccounted-for laptops are not at risk of unauthorized disclosure of PII.

Accuracy of Current DSS Property Accountability. As part of the audit, the audit team tested current DPAS records (including records of laptops and desktops) to determine their accuracy as of May 2007. Using the same inventory record system used to determine that DSS had 501 unaccounted-for laptops, we reviewed a random sample of 50 current DPAS property records and performed a book-to-floor and floor-to-book inventory to see if the DPAS records and the items in DSS staff members' possession matched. The audit team found that only 23 of the 50 records (46 percent) were accurate. As a result, the total of laptops unaccounted for, which DPAS records showed was 501, could be higher or lower because the DPAS records at DSS were not accurate.

---

[12] Directorate of Logistics is an activity within the Office of the Administrative Assistant to the Secretary of the Army responsible for providing logistics support to all DoD activities in the National Capital Region.

The audit team used the 501 unaccounted-for laptops as a baseline for the laptop search because it was the best information available when the audit began. See Appendix C for additional explanation of the testing performed at DSS.

Reporting of Possible Breaches to US-CERT and the Defense Privacy Office. In March 2007, the audit team met with an attorney from the office of the DSS General Counsel and with the Deputy Director of US-CERT to discuss the unaccounted-for laptops and to determine what steps DSS should take to comply with US-CERT reporting requirements. DSS contacted US-CERT and the Defense Privacy Office in March 2007. US-CERT and the Defense Privacy Office stated that, when DSS and the DoD IG audit team exhausted their search for the unaccounted-for laptops, DSS should report the incident to US-CERT and the Defense Privacy Office.

DSS reported the unaccounted-for laptops and mitigating information to the Defense Privacy Office on January 10, 2008.[13] According to the Director of the Defense Privacy Office, the risk of unauthorized disclosure of PII associated with the unaccounted-for laptops was not high enough to warrant a public notification of a breach of PII. The Director of the Defense Privacy Office added that, because there is no evidence that any of the laptops or hard drives left Government control, notifying the public of a breach would cause unnecessary alarm and panic. DSS also met with US-CERT on January 16, 2008, to report the unaccounted-for laptops and present additional information that DSS believes mitigates the risk of unauthorized disclosure of PII.

According to the DSS Deputy Director, after considering the factors outlined in the September 21, 2007, OSD Director of Administration and Management memorandum, DSS determined that there was little or no likelihood that a breach of PII had occurred. In making that determination, DSS considered there was no evidence any laptops or hard drives were stolen or ever outside of Government control. Moreover, through its ongoing search efforts, DSS continued to locate unaccounted-for laptops and hard drives, and DSS management believed that it ultimately would be able to account for all of the remaining laptops and hard drives. Because the risk of harm and the likelihood of the risk occurring were low, DSS determined that public notification of a potential breach would create unnecessary concern and confusion among those individuals who may be affected by the potential breach. Therefore, in accordance with OMB and DoD guidance, DSS concluded that public notification was not required.

Auxiliary Hard Drives

The DSS transition team agreed with OPM that DSS would purchase and permanently transfer an undetermined number of auxiliary hard drives for DSS PSI investigators transferring to OPM. The hard drives would afford access to OPM's Personnel Investigations Processing System software. Although no written agreement existed regarding the auxiliary hard drives, according to the DSS Chief of Support Services, the intent was to allow OPM to keep the hard drives. DSS and OPM personnel were unable to determine the number of auxiliary hard drives because, at the time of the transfer,

---

[13] On May 2, 2008, DSS provided the Defense Privacy Office with an updated briefing and provided the Director of Administration and Management an updated memo for a determination regarding public notification (see a scanned copy of the May 2, 2008, memorandum in the Management Comments section).

DSS did not maintain a record of the purchase of the hard drives nor log the assets in DPAS.

As further corroboration that the hard drives were intended to become permanent OPM assets, in June 2007, the OPM Deputy Associate Director provided the DoD IG audit team a memorandum certifying that:

> These secondary hard drives were not scheduled for return to DSS, and
> remained in the possession of OPM. OPM will continue to manage this as part
> of their equipment inventory, and will dispose of them when appropriate
> according to agency security standards.

The OPM certification, however, did not specify the number of auxiliary hard drives that DSS purchased and transferred to OPM. According to interviews with the OPM Deputy Associate Director and the former Acting Director at DSS, the auxiliary hard drives were used only to access the OPM Personnel Investigations Processing System and therefore did not contain PII collected at DSS. The hard drives contained PII related only to OPM investigations and are under OPM control and responsibility. Although DSS purchased the auxiliary hard drives, we have no indication that they were ever used to access anything but OPM systems. Therefore, based on the verbal agreement and the June 2007 OPM memorandum, OPM has accepted responsibility for the auxiliary hard drives and any PII on them. Consequently, DSS is not responsible for the information residing on the auxiliary hard drives.

CACs

In DoD, the Defense Manpower Data Center (DMDC) is responsible for managing and issuing CACs. DMDC issues CACs for use by personnel as both a form of identification to enter DoD facilities and a means of electronic authentication to obtain access to DoD computer systems. According to the DSS "Common Access Card Procedures Within Defense Security Service," January 2004, when DoD personnel leave DoD for a non-DoD agency, they must turn in their CACs. Thus, DSS should have collected the CACs from the personnel who transferred to OPM. In addition, according to the "Certificate Policy for United States Department of Defense, Version 9.0," February 9, 2005, issued by the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer (ASD[NII]/CIO), DoD civilian CACs must be electronically deactivated, meaning they can no longer be used to obtain access to DoD computer systems when an employee leaves DoD for a non-DoD agency. Thus, DSS should have contacted DMDC to deactivate the cards of the personnel who transferred to OPM.

According to the DSS Chief of Security, as part of the transfer, DSS allowed former DSS investigators to retain their CACs so they could access DoD facilities to complete ongoing security investigations. OPM employees were to return the CACs on March 19, 2005, 1 month after the transfer. However, 2 years after the transfer, 55 CACs[14] were still active. The Chief of Security, began working with DMDC and reconciling the

---

[14] In February 2008 DSS determined that OPM issued 7 of the 55 CACs to former DSS employees after they transferred to OPM.

CACs in July 2006. In February 2007, DMDC electronically deactivated all 55 remaining unauthorized CACs.

DMDC determined that there were 55 former DSS employees with outstanding CACs. DMDC records showed that, of 1,567 DSS employees that transferred to OPM, 276 had CACs at the time of the transfer. Of the 276 CAC holders, 221 were authorized to retain their CACs after their transfer to OPM because they were also either military reservists or were affiliated with another part of the military. The remaining 55 of the 276 CAC holders should have turned their CACs in to DSS when they transferred from DSS to OPM, and DSS should have notified DMDC to electronically deactivate the CACs.

Although all 55 CAC holders should have turned in their CACs at the time of the transfer, according to OPM and DSS records, 21 of the 55 unauthorized cardholders ended up gaining employment with other DoD agencies instead of OPM, and therefore were permitted to keep their CACs. OPM collected and destroyed another 21 of the 55 unauthorized CACs, and 6 of the employees exchanged their DoD CACs for affiliate (non-DoD) CACs. In February 2008 DSS determined the remaining seven CACs were issued to former DSS employees after they transferred to OPM and are the responsibility of OPM to collect.

As of May 2008, OPM management reported it had collected six of the seven CACs and was continuing efforts to retrieve the remaining unaccounted-for CACs. Table 4 shows the status of the cards.

Table 4. Status of 55 DoD Civilian CACs	
Status of CACs	Number of CACs
DoD rehired individual associated with CAC	21
OPM documented collection or destruction	21
Individual exchanged DoD CAC for affiliate CAC	6
CACs DSS is responsible for	48
Issued to former DSS employees after they transferred to OPM	7
Total	55

Safes

The DSS Chief of Security explained that the DSS transition team provided OPM a number of safes as part of the transfer of the PSI function from DSS to OPM. However, the Chief of Security could not provide the number of safes transferred to OPM because the transfer was based on a verbal agreement between the transition team and the Director at OPM.

In July 2007, the OPM Field Support Branch Chief provided the audit team a certification that OPM had received 23 safes from DSS during the transfer and that none of the 23 safes contained sensitive or classified information. The certification further stated that the safes did not contain any DoD sensitive or classified material while in the

possession of OPM. Although OPM has certified it received 23 safes, the fact that DSS cannot determine the number of safes transferred means there is a risk that additional safes remain outstanding and that sensitive or classified information contained in those safes is not under the control of either DSS or OPM. The DSS Chief of Security has stated that any unaccounted-for safes are not a security concern because (1) OPM certified that none of the safes transferred to OPM contained DSS sensitive or classified material and (2) the safes remained in DSS offices taken over by OPM and were never shipped to other locations. On the basis of these mitigating factors, we have determined no additional action is needed regarding potentially unaccounted-for safes.

Planning and Maintaining Accountability for DSS Assets

As of February 11, 2008, DSS could not fully account for 193 laptops by unique identifier because former DSS management did not:

- plan for the transfer of assets from DSS to OPM during the transfer of the PSI function;

- define property accountability requirements or oversee the contractor hired to collect and return DSS laptops lent to OPM; or

- maintain accurate property accountability records for safes, laptops, and auxiliary hard drives during and after the transfer of the PSI function to OPM in accordance with DoD Instruction 5000.64.

In addition, current DSS management has not fully implemented planned improvements to inventory accountability.

Planning for the Transfer of Assets From DSS to OPM. The former DSS management at the time of the transfer did not properly plan for the transfer of assets from DSS to OPM. The memorandum of understanding and memorandum of agreement only defined the reassignment of DSS personnel to OPM and specified an associated budget. The formal agreements did not indicate whether CACs, safes, laptops, and auxiliary hard drives would transfer to OPM or whether OPM would transfer any of the assets back to DSS.

Instead, according to the DSS Chief of Support Services, the former Directors of DSS and OPM based the transfer of hundreds of CACs, laptops, auxiliary hard drives and numerous safes on an informal, verbal agreement and did not document the number of assets that would transfer temporarily or permanently to OPM. In addition, according to the DSS Chief of Security, DSS management at the time of the transfer left key personnel including him out of the decision-making process. In addition, DSS at the time of the transfer did not fill the property book officer position when the previous property book officer transferred to OPM. By not properly planning and documenting the transfer of assets and responsibility for them, the former DSS and OPM Directors put the PII of military and civilian employees who were investigated for security clearances between 1997 and 2005 at risk. If even one laptop containing PII left the control of the Government and fell into the hands of unauthorized users, it could cause harm through identity theft or disclosure of PII. Because there was no formal

documentation, subsequent and current DSS managers have been unable, despite considerable efforts, to determine what assets changed hands, what assets were returned to DSS, or what assets may be outstanding. The fact that the assets were unaccounted for, coupled with the fact that they contained PII, created the risk of compromised PII.

Defining the Contractor's Property Accountability Requirements. On August 10, 2004, DSS entered into a $4.7 million contract with MZM Incorporated (MZM) to assist DSS in the transfer of the PSI function from DSS to OPM. Because DSS did not have a contracting officer, DSS used the Defense Information Systems Agency to award and administer the contract. The DSS Director of Administration and Management performed contracting officer representative responsibilities, including writing the statement of work and performing contract oversight. The contract required MZM to provide assistance in closing DSS field offices that carried out the PSI function, provide short-term storage of collected DSS assets, and then turn in the assets to the local DRMO. In addition, the statement of work listed the following requirements.

- Maintain the DSS laptop inventory until the final transfer of functions to OPM.

- Maintain inventory listings as required by the Government.

- Recommend disposition of nonserviceable items to the DRMO.

Although the contract tasked MZM to maintain the DSS laptop inventory and maintain inventory listings as required by the Government, the contract did not assign MZM responsibility for removing laptops from the DPAS inventory as they were disposed of at the DRMO, nor did the contract define what was required by the Government. Instead, the former DSS property book officer compensated for the lack of specific language in the statement of work by providing MZM access to DPAS and instructing MZM to remove the laptops from the DPAS inventory as MZM shipped the laptops to the DRMO for disposal or returned them to the DSS inventory.

In August 2004, MZM subcontracted the collection of laptops to Improsive Technologies (Improsive) while MZM kept the responsibility for closing field offices. Specifically, the statement of work listed the following requirements:

- Maintenance of DSS laptop inventory, and

- Disposition of nonserviceable equipment.

Like the MZM contract, the Improsive subcontract did not contain any language regarding the removal of laptops from DPAS, nor did the subcontract define the requirements for maintaining DSS laptop inventory or disposing of nonserviceable equipment.

Although the subcontract did not specify the removal of laptops from DPAS, again the former DSS property book officer provided Improsive access to DPAS and told Improsive to remove laptops from the DPAS inventory as Improsive collected them from OPM and sent them to the DRMO for disposal from August 13, 2004, to March 9, 2006.

According to an Improsive employee involved with the movement of laptops, as MZM closed field offices, MZM sometimes shipped laptops to the DRMO without recording their disposal in DPAS. We found documents signed by an MZM employee for 32 laptops that were turned in to the DRMO without being removed from DPAS records.

If DSS had performed proper planning before writing the statement of work and had taken into consideration the importance of removing laptops from DPAS records, it would have fewer unaccounted-for laptops. In addition, if DSS had performed adequate oversight of the contract with MZM, DSS might have become aware of MZM shipping laptops to the DRMO without making the appropriate entries in DPAS. DSS then might have been able to take corrective actions to maintain accountability.

Maintaining Accurate Records. DoD Instruction 5000.64 requires accountability and transaction trails throughout an asset's life cycle. The Instruction requires DoD Components to maintain accounting records of property lent to other Federal agencies, such as the laptops that DSS provided to OPM for the transfer of the PSI function.

Use of DPAS. DSS did not comply with DoD Instruction 5000.64 by not keeping accountable records of laptops provided temporarily to OPM, or keeping a transaction trail throughout the life cycle of the laptops, from acquisition to disposal. As a result, DSS, OPM, and the DoD IG audit team had to search through hundreds of DRMO documents and conduct searches of field offices to locate 308 of the 501 laptops.

DPAS is a DoD-wide property accountability system designed to track assets throughout their life cycle. DPAS provides an audit trail in accordance with DoD Instruction 5000.64, which requires that data elements such as unique identifiers be included in the property system of record. DPAS allows users to process accountable records by documenting receipts and turn-ins and tracking inventory. DSS lacked accurate records for the laptops because DSS did not consistently use DPAS to account for its laptops. Instead, DSS used a combination of DPAS and electronic spreadsheets. DSS used the electronic spreadsheets after its property book officer transferred to OPM, leaving no one with a working knowledge of DPAS. The electronic spreadsheets were not designed to capture information necessary to provide an audit trail, such as the specific person responsible for the laptop or the actual location of the laptop. For example, of the 308 laptops located, 41 were located at DSS headquarters but were initially listed as unaccounted for because entries for them were not in DPAS but on separate electronic spreadsheets.

Use of Unique Identifiers. According to the DSS Deputy Director, DoD Instruction 5000.64 does not explicitly require that laptops be tracked by a unique identifier. He is correct that DoD Instruction 5000.64 is not specific about laptops; however, it does state that items that are sensitive should be tracked by unique identifier. And because the Defense Privacy Office considers PII sensitive information, to be cautious, laptops should be tracked using a unique identifier. In fact, to clarify any misinterpretation that DoD Components may have regarding tracking laptops by unique identifier, the audit team met with a property accountability specialist in the Office of the USD(AT&L) and discussed clarifying DoD Instruction 5000.64 by explicitly stating that laptops must be tracked by unique identifier. The author of guidance in USD(AT&L) was agreeable to clarifying the guidance.

DSS turned in at least 122 laptops to the DRMO that could not be identified by unique identifier, in part because USD(AT&L) guidance did not require DoD Components to include unique identifiers on DRMO turn-in documents. Consequently, DSS did not always include unique identifiers on laptops they turned in to the DRMO. For example, one of the DRMO turn-in documents included 78 laptops without listing unique identifiers. Had USD(AT&L) required DSS to include unique identifiers on DRMO turn-in documents, DSS may have been able to provide clearer evidence that it disposed of the laptops through the DRMO.

Clarifying Guidance. Over the past 5 years, incidents involving the potential compromise of PII on laptops have become more prevalent in the Federal Government. For example, in 2002 the Federal Bureau of Investigation lost 317 laptops, resulting in a PII breach. In 2006, the Department of Veterans Affairs reported a breach of information related to a stolen laptop that contained PII on over 26.5 million veterans. According to the Department of Veterans Affairs, the cost of the breach could be as much as $500 million. As a result, it is imperative that DoD Components provide electronic protection and physical accountability, and know how to respond to a breach of PII. To address these issues, multiple DoD offices have issued clarifying policies. The ASD(NII)/CIO, USD(AT&L), and the OSD Director of Administration and Management have issued the following guidance on the electronic security, physical security, and notification of breaches of PII.

- On July 3, 2007, the ASD(NII)/CIO issued "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media Used Within DoD," which addresses encryption of sensitive information on mobile computing devices such as laptops.

- On November 2, 2006, USD(AT&L) issued DoD Instruction 5000.64, "Accountability and Management of DoD-Owned Equipment and Other Accountable Property," which addresses accountability for DoD-owned equipment.

- On September 21, 2007, the OSD Director of Administration and Management issued the memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," which addresses reporting breaches of PII.

To provide a seamless source of instruction on how to protect PII on mobile computing devices such as laptops, the ASD(NII)/CIO, the USD(AT&L), and the Director of the Defense Privacy Office met on August 29, 2007, to discuss the issuance of a memorandum to direct DoD managers to the proper guidance that will address all aspects of protecting sensitive and classified information on mobile computing devices. The Director of the Defense Privacy Office verbally agreed to take the lead on developing the guidance. However, a specific deadline for issuance of the guidance has not been established.

Current DSS Inventory. Current DSS management inherited inaccurate inventory records from previous management. However, at the time of this audit, current DSS management had not fully implemented planned improvements to inventory accountability. Based on a review of a sample of DSS inventory records, we determined the records remained inaccurate. Specifically, of the 50 DPAS employee custodial

records we reviewed, only 23 were accurate. The book-to-floor and floor-to-book inventory review performed by the audit team identified inventory items assigned to DSS employees that DSS could not locate. In addition, the audit team identified assets in the possession of DSS employees that DSS did not list in DPAS. Because of the long-standing inaccuracies in the DSS inventories, the reliability of the totals of unaccounted-for laptops and other assets remains in question.

Current DSS management recognizes that the agency's inventory records are not accurate and reported this as a weakness in the DSS "Memorandum for the Secretary of Defense FY 2007 Annual Statement Required Under the Federal Managers' Financial Integrity Act of 1982," August 20, 2007. Current DSS management listed the following objectives to improve accountability for agency assets.

- Finalize and implement DSS policy and procedures for all categories of plant, property, and equipment in first quarter of FY 2008.

- Complete inventory of DoD property held by OPM and update DPAS in first quarter of FY 2008.

- Complete inventory of all items classified as sensitive property and ensure items are properly accounted for in DPAS in accordance with DSS policy in second quarter of FY 2008.

- Certify DSS inventory of sensitive property in DPAS in third quarter of FY 2008.

- Verify that supporting documentation for reviews and inventories is generated and maintained in accordance with policy in third quarter of FY 2008.

Risk of Compromised PII

Accountability for assets such as CACs, safes, laptops, and auxiliary hard drives that contain PII is critical to reduce the risk that those assets can be compromised and the information used inappropriately. During the transfer of the PSI function from DSS to OPM in February 2005, DSS management did not define the parameters for transferring the assets to OPM along with 1,567 former DSS staff members. And during the transfer, DSS did not take the necessary steps to accurately account for the assets. DSS management since the transfer has not completed steps to improve asset accountability. As a result, at the outset of this audit, DSS could not account for at least 55 CACs, [15] 501 laptops, and an undetermined number of safes and auxiliary hard drives. Since then DSS has been able to resolve the 55 CACs, show evidence that the 501 laptops had not left Government control, and perform significant due diligence to resolve accountability issues related to unaccounted-for safes.

---

[15] In February 2008 DSS determined that OPM issued 7 of the 55 CACs to former DSS employees after they transferred to OPM.

Laptops. Although at the beginning of the audit DSS could not locate 501 laptops, the efforts of DSS, OPM, and the DoD IG resulted in physically locating 308 laptops, and accounting for the remaining 193 by other means as of May 2008. DSS management in place during the transfer created a lack of accountability for assets, posing an undue risk of compromising PII for military, civilian, and contractor employees investigated for personnel security clearances between 1997 and 2005. To date, no evidence has come to light to indicate that the laptops have left the Government or that PII has been compromised. Still, the potential for compromise occurred. For example, in October 2007 DSS located 14 laptops in a secured, caged area of a commercial storage facility in California used by MZM while closing DSS field offices. However, neither DSS nor MZM had paid the monthly storage fees in over a year, and DSS has no proof that those 14 were the only laptops placed in the storage facility. It is unclear whether DSS has had full control over all its laptops and the PII contained on them.

Of further concern is the extent of PII maintained on the laptops. The audit team performed a forensic review on a sample of the recovered laptops. We determined that data contained on the hard drives was easily accessible without a password. Based on a limited review of 33 recovered hard drives, the audit team found PII ranging from as early as 1997 to as late as 2005. Although the DoD IG audit team found no evidence of compromised PII, the lack of accountability caused by DSS management in place during the transfer posed a risk of compromising PII of military, civilian, and contractor employees. However, continued efforts by DSS current management have shown the remaining unaccounted-for laptops have not left the Government, reducing the risk of compromise of PII on those devices to low or none.

CACs. In February 2005, DSS allowed 55 DSS employees to leave DoD without collecting and deactivating the employees' CACs. However, in July 2006, once made aware of the issue, DSS did take steps to have DMDC deactivate all 55 CACs. DSS and DMDC took steps to deactivate all 55 outstanding CACs, of which DSS and OPM collected 48. The remaining seven CACs were issued to former DSS employees after they had left DSS and therefore are OPM's responsibility to collect.

Safes. According to the DSS Chief of Security, DSS could not determine the number of safes transferred to OPM. However, the OPM Chief of Field Support Services certified that OPM received 23 safes and that the safes did not contain any DoD sensitive or classified information while they were in the possession of OPM.

To determine the accuracy of the current inventory of DSS safes, we performed a review at DSS headquarters and DSS field offices.[16] Although DSS could not determine the number of safes it transferred to OPM, the DSS inventory records at the time of our review matched the physical inventory at headquarters in Alexandria, Virginia, and at field offices in Chantilly, Virginia; Huntington Beach, Pasadena, San Diego, and Sunnyvale, California; and Linthicum, Maryland. The Chief of Security has ultimate responsibility for safes at DSS and is working with the DSS property book officer to update DPAS records to include a DSS-wide inventory of safes.

Internal Controls Over DSS Assets. DSS continues to experience difficulties in accounting for assets that were not part of the transfer to OPM. Specifically, only

---

[16] The DoD IG inventory review of safes was performed separately from the DoD IG inventory review of laptops and desktops in DPAS.

46 percent of DPAS records of laptops and desktops we reviewed were accurate. DSS must improve controls over and accountability for assets currently in its possession. Although it is clear that DSS inherited inaccurate accounting records, DSS is responsible for putting controls in place that will help ensure property accountability.

Actions Taken by DSS

Current DSS management has worked diligently to account for the unaccounted-for assets, particularly the laptops that potentially contained PII. Through joint efforts, 308 of an estimated 501 laptops have been located and confirmed by unique identifier. DSS has obtained evidence that the remaining 193 laptops have remained in Government control. Although some risk exists because the initial baseline of 501 laptops was not accurate, DSS has worked with Defense Privacy Office and US-CERT officials, who have concluded that because of DSS continued efforts, the risk of unauthorized disclosure of PII is not high enough to warrant a public notification of a breach of PII. In addition, DSS demonstrated that as of February 2007 all 55 CACs had been deactivated, and as of February 2007, the remaining CACs that were the responsibility of DSS had been physically collected.

Current DSS management inherited a property accountability process that lacked adequate internal controls. We commend DSS management for taking steps to improve controls over property accountability. Specifically, in spring 2007, DSS began reconciling DPAS records and issuing hand receipts for DSS assets including laptops. In addition, the property book officer wrote new draft guidance that requires DSS to perform a physical inventory every year. This requirement is more stringent than DoD Instruction 5000.64, which requires DoD Components to perform a physical inventory every 3 years. DSS began performing an inventory review in August 2007, and managers continued to gather information through May 2008. They showed with reasonable certainty that the remaining unaccounted-for laptops have not left the control of the Government and that the risk of unauthorized disclosure of PII is reduced.

In response to the draft report, the Director stated DSS management continued to improve inventory records at DSS by conducting regular inventories that included a 100-percent inventory between March and December 2007. The Director also stated DSS implemented new procedures for procuring, receiving, and accounting for property. The procedures include capturing all information technology equipment in DPAS. The Director further stated she added a team leader and five support staff to DSS Support Services, the office responsible for keeping accurate property records. In addition, DSS management is preparing an operating instruction that will accompany DSS Regulation 15-2, "Property Management."

Management Comments on the Finding and Audit Response

Please see Appendix D for management comments and audit responses on the finding.

Recommendations, Management Comments, and Audit Response

Revised, Deleted, and Renumbered Recommendations. As a result of new evidence provided by DSS management that showed the remaining 7 of the 501 initially unaccounted for laptops had not left the control of the Government; and the remaining 7 unaccounted for common access cards were issued to former DSS employees after they left DSS, we have deleted draft Recommendations 1.f.,1.g.,1.h. In addition, based on mitigating risk factors related to potential unaccounted for safes we removed recommendation 1.i. and renumbered the other parts of Recommendation 1. accordingly. We also revised Recommendation 3. to clarify its intent.

1. We recommend that the Director, Defense Security Service assign appropriate personnel to:

   a. Maintain an audit trail showing all transactions from acquisition to disposal for assets that contain sensitive or classified information in accordance with DoD Instruction 5000.64, "Accountability and Management of DoD-Owned Equipment and Other Accountable Property," November 2, 2006.

Management Comments. The Director, Defense Security Service concurred and explained that the DSS Property Management Regulation became effective on February 8, 2008. The regulation assigns responsibilities at all levels for the management and accountability of DSS assets throughout each asset's life cycle. In addition, DSS management is developing Property Management Operating Instructions that further define processes and procedures for accountability and management of DSS property, plant, and equipment. The Director expects to publish the operating instructions in the third quarter of FY 2008. Finally, the Director stated that on March 31, 2008, she had detailed a full-time employee to help integrate the Chief Information Officer inventory spreadsheet into DPAS and provide guidance to the Chief Information Officer for the life-cycle management of and accountability for information technology assets.

Audit Response. The Director, Defense Security Service comments were responsive. Developing and implementing the DSS Property Management Regulation and Operating Instructions, combined with conducting physical inventories as discussed in Recommendation 1.b., will help DSS maintain an audit trail in accordance with DoD Instruction 5000.64. No additional comments are needed.

   b. Conduct a periodic physical inventory of laptops and other assets that contain personally identifiable information.

Management Comments. The Director, Defense Security Service concurred and explained that, in addition to requiring a 100-percent physical inventory of all DSS

property, plant, and equipment, DSS will also perform random spot inventories, verifying hand receipts and physical equipment. DSS management is seeking vendors that conduct physical inventory services and plans to have the first inventory reconciliation completed and property books transferred to a new property book officer in the first quarter of FY 2009.

Audit Response. The Director, Defense Security Service comments were responsive. The actions taken and planned meet the intent of the recommendation, and no additional comments are needed.

c. Track assets that contain personally identifiable information using a unique identifier, such as a serial number or bar code.

Management Comments. The Director, Defense Security Service concurred and plans to track all assets that could contain PII by using a serial number and barcode in DPAS throughout the assets' life cycle.

Audit Response. The Director, Defense Security Service comments were responsive. The actions taken by the Director meet the intent of the recommendation, and no additional comments are needed.

d. Report any future confirmed or unconfirmed instances of unauthorized disclosure of personally identifiable information to U.S. Computer Emergency Readiness Team and the Defense Privacy Office in accordance with Office of Management and Budget memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," July 12, 2006, and with DoD Directive 5400.11-R, "DoD Privacy Program," May 14, 2007.

Management Comments. The Director, Defense Security Service concurred, stating DSS would continue to comply with Office of Management and Budget and DoD requirements for potential breach or compromise of PII.

Audit Response. The Director, Defense Security Service comments were responsive, and no additional comments are needed.

e. Establish guidelines and training that DSS employees must follow to protect personally identifiable information from unauthorized disclosure.

Management Comments. The Director, Defense Security Service concurred, stating DSS would create PII protection training and make it part of the DSS New Employee Orientation Program. DSS will also include protection of PII as an annual training requirement. DSS expects to have the first training iteration ready by June 30, 2008.

Audit Response. The Director, Defense Security Service comments were responsive. The actions taken by DSS meet the intent of the recommendation, and no additional comments are needed.

f. Issue guidance that requires Defense Security Service to perform a physical inventory every year in compliance with DoD Instruction 5000.64.

Management Comments. The Director, Defense Security Service concurred. She stated that DSS Regulation 15-2, "Property Management," took effect on February 8, 2008. She said the guidance would be supplemented with more specific processes and procedures in the near future.

Audit Response. The Director, Defense Security Service comments on the recommendation were responsive. The actions taken and planned by DSS meet the intent of the recommendation, and no additional comments are needed.

2. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics:

a. Add clarifying language to DoD Instruction 5000.64 stating that the policy applies to mobile computing devices, including but not limited to laptops, mobile information storage devices, and auxiliary hard drives, regardless of dollar thresholds.

Management Comments. The Director, Acquisition Resources and Analysis, responding for the Under Secretary of Defense for Acquisition, Technology, and Logistics, concurred. She stated that DoD Instruction 5000.64 will be revised to clarify property accountability and management guidance for information technology property items that contain personally identifiable information.

Audit Response. Management comments were responsive, and no additional comments are needed.

b. Require that all DoD Components include unique identifiers on Defense Reutilization and Marketing Office turn-in documents when disposing of laptops and other electronic devices that may contain personally identifiable information.

Management Comments. The Director, Acquisition Resources and Analysis, responding for the Under Secretary of Defense for Acquisition, Technology, and Logistics, partially concurred. She stated that they agree with the objective and intent of the recommendation. However, she suggested that guidance in two documents not captured in the report may eliminate the need for the recommendation. The documents are:

- Deputy Secretary of Defense Directive Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," May 29, 2001; and

- Assistant Secretary of Defense for Command, Control and Communications Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001.

These two memoranda require that all hard drives of unclassified computer equipment leaving the custody of DoD be sanitized and certified that the sanitization process occurred.

Audit Response. Management comments were not responsive. Although the two memoranda listed above address the removal of information from hard drives and the destruction of hard drives, the memoranda do not address accountability for DoD

laptops as they are turned in to the DRMO for disposition. Therefore, the two memoranda do not meet the intent of the recommendation.

Requiring DoD Components to list unique identifiers (serial numbers) on DRMO turn-in documents would complete the transaction trail, showing evidence the laptop was properly disposed of. Conversely, not listing laptops by unique identifier on the DRMO turn-in document makes it impossible to document that specific laptops were turned in to the DRMO. For example, DSS and the DoDIG audit team reviewed turn-in documents showing 65 laptops were disposed of at DRMO locations. However, DSS could not clearly determine whether the laptops were part of the 501 unaccounted-for laptops because the DRMO turn-in documents lacked a unique identifier. We request that the Under Secretary of Defense for Acquisition, Technology, and Logistics reconsider his position on Recommendation 2.b. and provide additional comments in response to the final report.

3. We recommend that the Director of the Defense Privacy Office continue working with the Office of the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer and the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics to issue a memorandum to all DoD managers identifying all guidance pertaining to protecting personally identifiable information, responding to breaches of personally identifiable information, and accounting for assets.

Management Comments. The Senior Agency Official for Privacy did not concur with the draft recommendation that the Defense Privacy Office continue working with the Office of the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer and the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics to develop overarching guidance on the protection of PII on mobile computing devices because such guidance would only confuse them.

Audit Response. Based on management comments, we revised the draft recommendation to develop overarching guidance. The intent of the recommendation was not to reissue or rewrite or even summarize existing guidance, but to tell DoD managers which guidance they should follow when protecting PII, accounting for assets that are sensitive, and reporting a potential breach of PII. The purpose of the memorandum is to have one document that directs DoD managers to all the proper guidance for electronic protection, accountability, and reporting of breaches—guidance that has been written by different DoD Components. The memorandum would help ensure that DoD managers are aware of and follow all the proper guidance and procedures when handling PII and sensitive assets. We request that the Director of the Defense Privacy Office respond to the revised recommendation in comments on the final report.

Appendix A. Scope and Methodology

We conducted this performance audit from November 2006 through May 2008 in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We reviewed DSS controls over assets that contain sensitive personal data or PII. For purposes of this audit, assets included laptops, hard drives, CACs, and safes. We interviewed DSS and OPM personnel involved with the transfer of the PSI function to OPM to determine the procedures they used to account for laptops, hard drives, CACs, and safes transferred. We exhausted all leads stemming from these interviews in our search to account for the unaccounted-for laptops, CACs, and safes. Additionally, we performed a book-to-floor-inventory and floor-to-book-inventory to evaluate the reliability of DSS records of current assets.

Laptops. We interviewed the former DSS Chief of Support Services, former Improsive personnel, the former DSS Assistant to the former Acting Director, the DSS Supply Management Specialist, the former DSS Property Manager, and former DSS Acting Directors to find out what happened to the laptops during the PSI function transfer. We reviewed documentation from DSS and OPM personnel to determine possible locations of laptops. We reviewed turn-in documents to identify those laptops transferred to other agencies. We coordinated with the OPM Deputy Associate Director to obtain certifications from DSS employees who became OPM employees as to the status of their laptops. We reviewed the certifications to determine the last known individual and /or location associated with each laptop and followed each piece of information until we exhausted all leads.

To search for unaccounted-for laptops, we conducted site visits to DSS offices in Alexandria and Chantilly, Virginia; Smyrna, Georgia; Huntington Beach, Pasadena, San Diego, and Sunnyvale, California; Columbus, Ohio; and Linthicum, Maryland. We also coordinated with the OPM Chief of Internal Audits Group to visit OPM locations in Boyers, Pennsylvania; Long Beach, California; Ft. Meade, Maryland; Smyrna, Georgia; St. Louis, Missouri; and Virginia Beach, Virginia.

We coordinated with the Defense Criminal Investigative Service to search pawn shops in cities identified as having the most unaccounted-for laptops. Investigators searched pawn shops in the District of Columbia metropolitan area and in Maryland, Texas, California, Florida, and Virginia.

We judgmentally selected a sample of 33 hard drives pulled from located laptops that were originally included in the 501 unaccounted-for computers. The DoD IG Defense Criminal Investigation Service performed a forensics review of the 33 hard drives to determine whether they contained PII. Seventeen of the thirty-three hard drives did contain PII.

CACs. We interviewed the DSS Chief of Security to determine the procedures used to account for, collect, and terminate the CACs issued to PSI agents who transferred to OPM. We verified the information with DMDC and the OPM Chief of Field Support.

Safes. We interviewed the DSS Chief of Support Services, the DSS Chief of Security, and the OPM Federal Investigative Services Program Manager to account for safes transferred from DSS to OPM and to determine what controls DSS has in place over safes.

Policy. We reviewed DoD policies, regulations, and guidance applicable to property accountability and the safeguarding of assets and sensitive information. We interviewed officials from ASD(NII)/CIO, Department of Homeland Security, USD(AT&L) and the DoD Privacy Office to determine additional criteria applicable to property accountability, security of assets, and incident reporting.

Use of Computer-Processed Data. We used computer-processed data from DPAS to identify the 501 laptops that DSS could not account for. Our review of DPAS records indicated that property records in DPAS were not always accurate; therefore, we cannot be certain that 501 is the correct number of unaccounted-for laptops at DSS. We used computer-processed data from the Defense Enrollment Eligibility Reporting System to identify the CACs that DSS could not account for. We did not assess the reliability of the data from the Defense Enrollment Eligibility Reporting System, but have no reason to suspect that the data are inaccurate.

Scope Limitation. We obtained information from DSS that indicated as many as 193 laptops that were other than physically accounted for were not at risk of unauthorized disclosure. Although we documented the DSS methodology for obtaining the information, because we obtained the information after we completed our fieldwork, we did not verify all of the supporting data.

Use of Technical Assistance. We obtained assistance from our Quantitative Methods Division in selecting a sample of DPAS records to assess the accuracy of the DSS property inventory.

Government Accountability Office High-Risk Area. The Government Accountability Office has identified several high-risk areas in the Department of Defense. This report provides coverage of the business transformation high-risk area specifically, the security clearance program and contract management.

Appendix B. Prior Coverage

During the last 5 years, the Government Accountability Office (GAO) and DoD IG have issued 7 reports related to adequate controls and accountability to secure assets that contain sensitive personal information. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/audit/reports.

GAO

GAO Report No. GAO-06-1070, "DoD Personnel Clearances: Additional OMB Actions Are Needed to Improve the Security Clearances Process," September 2006

GAO Report No. GAO-06-706, "Managing Sensitive Information: DoD Can More Effectively Reduce the Risk of Classified Errors," June 2006

GAO Report No. GAO-05-207, "High-Risk Series: An Update," January 2005

DoD IG

DoD IG Report No. D-2003-112, "Contracting Practices of the Defense Security Service for Personnel Security Investigations," June 27, 2003 (For Official Use Only)

DoD IG Report No. D-2003-066, "Information System Security Controls Over the Use and Protection of Social Security Numbers Within DoD," March 21, 2003

DoD IG Report No. D-2003-036, "Supply Inventory Management Property Accountability at Research, Test, and Evaluation Installations," December 16, 2002

DoD IG Report No. D-2002-138, "Security Allegations Concerning the Management and Business Practices of the Defense Security Service," August 9, 2002

Appendix C. Review of Defense Property Accountability System Records

At the outset of the audit, DSS officials informed the audit team that they could not account for 501 laptops out of a universe of 2,826, of which 1,483 were transferred to OPM and used for PSIs. According to DPAS records, DSS could not account for 501 laptops, leaving 2,325 accounted for. To check for accuracy, the audit team randomly sampled 50 DPAS records. We ran a floor-to-book and book-to-floor review to see whether the information technology items (including laptops and desktops) listed for the individuals in DPAS records matched the items that those individuals maintained in their custody.

Only 23 of the 50 (46 percent) records in DPAS matched with what DSS personnel had in their possession. Included in the 50 DPAS records we reviewed were 7 of the 2,325 laptops that DSS should be able to account for. However, DSS accurately recorded only five of the seven laptops in DPAS. Specifically, two laptops were located on the floor but were not accurately listed in DPAS.

Because of the inaccuracies found in DPAS, we cannot be certain that 501 is the total unaccounted-for DSS laptop inventory.

Appendix D. Management Comments on the Finding and Audit Response

The Director, Defense Security Service provided comments on the finding that addressed accountability of laptops, CACs, and safes.[17]

Laptops

The Director, Defense Security Service provided comments on the following:

- compliance with DoD Instruction 5000.64,
- accounting for DSS laptops,
- risk associated with unaccounted-for laptops, and
- public notification.

Management Comments on Compliance With DoD Instruction 5000.64. The Director, Defense Security Service stated that the audit team is holding DSS to a higher standard than the rest of DoD by requiring serial number accountability. The Director, Defense Security Service pointed out that DoD Instruction 5000.64 states:

Accountable property records shall be established for all property purchased, or otherwise obtained, having a unit acquisition cost of $5,000 or more; leased assets (capital assets) of any value; and assets that are sensitive or classified.

DoD Instruction 5000.64 references DoD Manual 4100.39-M, Volume 10, Table 61 (Reference (k)), which lists examples of sensitive items—such as nonnuclear missiles and rockets; arms, ammunition, and explosives; drugs and other controlled substances; and precious metals—but does not list laptops that contain PII. Furthermore, the Director noted, DoD Instruction 5000.64 defines sensitive items as property requiring a high degree of protection and control due to statutory requirements or regulations. Nowhere in DoD Instruction 5000.64, she stated, is there a requirement that DoD Components track information technology equipment or other items containing PII by serial number or other unique identifier. The Director stated that not all laptops in DSS or DoD contain PII; therefore, not all laptops should be required to be tracked by unique identifier.

Audit Response. Officials from the Office of the USD(AT&L) stated that the intent of DoD Instruction 5000.64 is that DoD managers should consider their specific circumstances and use prudent judgment in determining what assets they should account for by unique identifier. Because 249 of the 501 initially unaccounted-for laptops at DSS were used for PSI investigations and may have contained PII, DSS managers should have accounted for these assets in a manner that would allow them to determine from their property records where each laptop is, and who is responsible for it at all times. Without accounting for laptops by unique identifier, it is extremely difficult for management to determine what laptops are missing and what laptops are accounted for.

---

[17] We considered the comments made by the Director on the finding discussion and made appropriate adjustments.

For example, DSS management spent approximately 3 years and significant resources to account for laptops and demonstrate they had not left the control of the Government. If DSS had implemented controls including accounting for laptops using unique identifiers during the transfer, DSS management could have tracked down the 501 initially unaccounted-for laptops faster and with fewer resources. The Director made the point that not all laptops at DSS contain PII; therefore, DSS should not have to account for all its laptops by unique identifier. However, because DSS lacked controls to demarcate which laptops contained PII, and any laptops can contain PII, DSS should account for all its laptops by unique identifier.

Furthermore, both the 2002 version of DoD Instruction 5000.64, paragraph 5.3.1.1, and the 2006 version, paragraph 6.3, state:

> Although the Department of Defense may not have physical custody, to maintain effective property accountability and control and for financial reporting purposes, DoD components shall establish records and maintain accountability for property (of any value) furnished to contractors as Government Furnished Property. This requirement includes property that is loaned and/or otherwise provided to outside entities such as Federal agencies, State and local governments, and foreign governments.

To maintain this accountability, the 2002 version[18] specifically lists data elements applicable to property accountability records and systems in paragraph 5.3.3.8 to be "part number, National Stock Number, serial number, bar codes, or other unique identifiers." The audit team used serial numbers as the unique identifier to account for laptops because we found from reviewing the DSS DPAS inventory records that serial numbers were the only consistent unique identifier used by DSS. Therefore, the audit team was not holding DSS to a higher standard, but used what DSS records had available to clearly identify the unaccounted-for laptops. The overall purpose was to physically verify the specific missing devices, and serial number, of all unique identifiers, was found to be the best data element in this case.

Management Comments on Accounting for DSS Laptops. The Director stated that the audit team mischaracterized the accountability standard of unique identifier by identifying 193 laptops as not fully accounted for. The Director further stated the audit team considered laptops fully accounted for only when the team obtained a scanned copy of the back of the laptop, a DD Form 1348-1 with a serial number, or a DA Form 3161 with a serial number. The Director pointed out that the draft audit report acknowledged that DSS further accounted for 186 of the remaining 193 laptops. The Director noted that DSS was able to coordinate with OPM and use a "new investigative methodology" to account for the remaining seven previously unaccounted-for laptops.

The Director stated that, prior to receiving the draft report, DSS had accounted for 186 of the 193 laptops using a "naturally progressive investigation." Although DSS initially attempted to meet the standard set by the DoD IG by accepting only scanned copies of the laptops, DD forms 1348-1A, and DA forms 3161 as serial number identification, DSS management finally used a standard of "reasonable degree of certainty" to

---

[18] The 2002 version of DoD Instruction 5000.64 was the version applicable during the transfer of the PSI function from DSS to OPM, which occurred in February 2005.

demonstrate that the PII contained on the laptops was properly disposed of or safeguarded.

Finally, the Director noted that DSS had been able to account for the remaining 7 of the 501 initially unaccounted-for laptops after the audit team issued the draft report. DSS staff accounted for the remaining laptops by comparing the laptop serial numbers entered on DRMO turn-in documents with the serial numbers entered in DPAS. DSS found that seven of the serial numbers listed on the turn-in documents were never entered in DPAS. Additional analysis showed that the seven laptops were each one digit off from the seven remaining unaccounted-for laptops listed in the property records. The Director concluded that the difference in the serial numbers may have been caused by data entry errors, which have since been corrected; therefore, DSS has accounted for the previously unaccounted-for laptops.

Audit Response. The audit team did not mischaracterize DoD Instruction 5000.64. The intent of the Instruction is that DoD managers should assess their specific circumstances and use prudent judgment in determining what assets they should account for using an unique identifier. Considering that 249 of the previously unaccounted-for DSS laptops potentially contained PII including financial, medical, and other personal information of military and civilian employees who were investigated for personnel security clearances between 1997 and 2005, prudent management should have accounted for these laptops in a manner that would allow it to verify the location and existence of each laptop. Accurate property records that use unique identifiers to track laptops enable management to have that level of control over the property accountability of laptops.

The Director's assessment of how the audit team determined a laptop was fully accounted for was not completely accurate. The audit team determined the laptop was fully accounted for if DSS could verify the existence of the laptop or could fully confirm its disposal. Because of the sensitive nature of PII on the laptops, the audit team differentiated between laptops that were fully accounted for and laptops that could be accounted for by a standard of reasonable certainty. We determined laptops were fully accounted for if we could physically locate them or verify documentation of their disposal through a DoD turn-in document. The auditors documented the existence of the laptops by scanning the unique identifier (serial number or barcode) on the back of the laptop, or documenting the disposal of the laptop by obtaining a copy of the DoD turn-in document and verifying the unique identifier listed on the document. The audit team considered unique identifiers other than serial numbers; however, at DSS, serial numbers were used because DSS had not consistently used any other unique identifier for the laptops. The audit team acknowledged in the audit report that DSS was able to account for the remaining 193 unaccounted-for laptops using a reasonable degree of certainty.

We reviewed the methodology DSS used to account for the remaining 7 of the 501 unaccounted-for laptops and obtained supporting documentation. We agree with the DSS conclusion that the remaining seven unaccounted-for laptops may be attributed to data entry errors. Therefore, we have deleted the draft recommendations for DSS to continue working with OPM to locate the remaining unaccounted-for laptops and to implement steps to mitigate the risk of unauthorized disclosure of the personally identifiable information stored on those laptops.

Management Comments on Risk Associated With Unaccounted-for Laptops.
According to the Director, DSS management has been able to show with a reasonable
degree of certainty that the risk of unauthorized disclosure of PII is low to nonexistent.
The Director emphasized that neither DoD IG audit team nor DSS investigators found
any evidence of theft or malicious intent regarding the unaccounted-for laptops. In
addition, the Director stated that DSS had properly disposed of more than 5,600 hard
drives and more than 1,800 laptops in accordance with DoD regulations. Further, the
Director stated that, of the 33 hard drives the audit team reviewed, only 17 contained
PII, and many of those hard drives contained PII of DSS agents, not the PII of the
subjects of security clearance investigations.

Audit Response. While we do not dispute that there has been no indication of theft or
malicious intent regarding the unaccounted-for laptops, or that DSS has properly
disposed of thousands of laptops and hard drives, some risk still exists because the
initial baseline of 501 laptops was not accurate. As a result, additional unaccounted-for
laptops may still exist. We also do not dispute that DSS followed National Security
Agency guidance or that DSS reviewed internal procedures for reformatting, storing,
and disposing of hard drives. However, we disagree that the risk is eliminated because
much of the PII on the hard drives tested belonged to DSS agents rather than to the
subjects of security investigations. PII of DSS agents requires the same level of
protection as that of the subjects they are investigating.

Management Comments on Determination of Public Notification. The
Director, Defense Security Service determined public notification was not
necessary in accordance with DoD Regulation 5400.11-R, "Department of
Defense Privacy Program," May 14, 2007, and the Director of Administration
and Management Memorandum, "Safeguarding Against and Responding to the
Breach of Personally Identifiable Information," September 21, 2007.
Specifically, DSS considered a two-part test, which included assessing (1) the
likely risk of harm and (2) the relative likelihood of the risk occurring. In
determining the likely risk of harm, DSS considered the following five factors
in accordance with the memorandum:

- the nature of the data elements breached,
- the number of individuals affected,
- the likelihood that the information is assessable and usable,
- the likelihood that the breach may lead to harm, and
- the agency's ability to mitigate the risk of harm.

According to the Director, Defense Security Service, when determining whether
notification was necessary, she took into consideration not only the five factors but also
that there was no evidence that any of the laptops were stolen or outside control of the
Government. Furthermore, the Director considered that, ultimately, DSS would be able
to account for the remaining unaccounted-for laptops. The Director, Defense Security
Service informed the Defense Privacy Office of its determination in a memorandum
dated January 15, 2008. The Defense Privacy Office agreed with the DSS
determination.

Audit Response. We agree that the Director, Defense Security Service, working with the Defense Privacy Office, made the determination that public notification was not warranted. The Defense Privacy Office has the authority to work with DoD Components to make the decision on public notification.

CACs

Management Comments on CACs. The Director, Defense Security Service stated the DSS Security Office began reconciling DoD CACs in July 2006. The Director further stated that OPM issued the seven remaining outstanding CACs after the employees transferred to OPM. Consequently, DSS is not responsible for retrieving the outstanding CACs. The Director, Defense Security Service added that OPM has since obtained six of the seven outstanding CACs and is continuing its efforts to locate the remaining CAC.

Audit Response. As result of management comments and additional work, we deleted the draft recommendation on CACs.

Safes

Management Comments on Safes. The Director stated that DSS received a final accounting of safes from OPM, certifying that DSS transferred 23 safes to OPM. The OPM certification stated that none of the safes contained sensitive or classified information and that all the safes were transferred to OPM but remained in place. The Director also pointed out that DSS and OPM conducted a thorough search and documented receipt of all known safes. The Director also stated that since the DoD IG audit, DSS has implemented enhanced control measures to account for safes, including assigning barcodes and entering information on safes in DPAS.

Audit Response. After further consideration of the due diligence performed by DSS and other mitigating factors, we determined that no additional action is necessary and deleted the draft recommendation to receive a final accounting of safes from OPM. We commend DSS for tagging all safes with unique identifiers in the form of bar codes and including safes in their official property records.

Appendix E. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense for Intelligence
Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief
    Information Officer
Director, Defense Privacy Office

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Naval Inspector General

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)

Other Defense Organizations

Director, Defense Security Service

Non-Defense Federal Organization

Office of Personnel Management

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Homeland Security and Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Oversight and Government Reform
House Subcommittee on Government Management, Organization, and Procurement,
    Committee on Oversight and Government Reform
House Subcommittee on National Security and Foreign Affairs,
    Committee on Oversight and Government Reform

Under Secretary of Defense for Acquisition, Technology, and Logistics Comments

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION,
TECHNOLOGY
AND LOGISTICS

APR 0 7 2008

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL AND DIRECTOR, DEFENSE FINANCIAL AUDITING SERVICE, DoDIG

SUBJECT: Response to DoDIG Draft Report on "Accountability for Defense Security Service Assets With Personally Identifiable Information" (Project No. D2007-D000LC-042.000)

As requested, I am providing responses to the general content and recommendations contained in the subject report.

Recommendations 2.a:
We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics revise the DoD Instruction 5000.64 to include clarifying language to DoD Instruction 5000.64 stating that the policy applies to mobile computing devices, including but not limited to laptops, mobile information storage devices, and auxiliary hard drives, regardless of dollar threshold.

Response: Concur. We agree with the objective and intent of this recommendation. The DoD Instruction 5000.64 will be revised to clarify property accountability and management guidance for Information Technology property items that contain personally identifiable information.
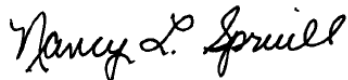
Recommendation 2.b:
We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics require that all DoD Components include unique identifiers on Defense Reutilization and Marketing Office (DRMO) turn-in documents when disposing of laptops and other electronic devices that may contain personally identifiable information.

Response: Partial Concur. We agree with the objective and intent of this recommendation. However, the following information regarding safeguards against compromise of personally identifiable information was not captured in the audit and may eliminate the need to take the recommended action. The Deputy Secretary of Defense Directive Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," dated May 29, 2001 (attachment 1), and Assistant Secretary of Defense for Command, Control and Communications Memorandum, "Disposition of Unclassified DoD

Computer Hard Drives," dated June 4, 2001 (attachment 2), identify that all hard drives of unclassified computer equipment leaving the custody of DoD are to be sanitized (overwritten, degaussed or destroyed). A certification process, which included documentation of the completion of sanitization actions, is also prescribed. In addition, all new contracts initiated after September 30, 2001 are directed to comply with this guidance. Based on the authoritative emphasis and detail instructions provided in these memoranda, current policy meets the intent of this recommendation. Hard drives are required to be sanitized and documentation affixed to the hard drive or computer housing device, prior to turn-in to the DRMOs. Therefore, we believe existing DoD policy and procedures meet the intent of this recommendation.

Please contact Ms. Sarah Ball, who can be reached at 703-604-6350 x103, or via email at sarah.ball@osd.mil, if additional information is required.

Nancy Spruill
Director, Acquisition Resources
and Analysis

Attachments:
As stated

Director of Administration and Management Comments

OFFICE OF THE SECRETARY OF DEFENSE
1950 DEFENSE PENTAGON
WASHINGTON, DC 20301-1950

ADMINISTRATION AND
MANAGEMENT

1 2 MAY 2008

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL
(DoD IG)

Subject: Draft IG Audit - Accountability of Defense Security Service Assets
with Personally Identifiable Information (PII)

I appreciated the opportunity to review and comment on your draft audit report of the Accountability for Defense Security Service Assets With Personally Identifiable Information, Project No. D2007-D000LC-0042.000, dated March 4, 2008. Except as noted below, I generally concur with your findings.

It is noted that the Defense Security Service (DSS) has performed a detailed and thorough forensic analysis of a significant number of laptops and a greater number of individual hard drives in an effort to recover those units involved in the functional transfer of security clearance investigation responsibility to the Office Personnel Management (OPM). I note that the DSS has completed the extensive search and analysis of hard drives and has identified hard drives determined to be associated with the functional transfer of laptops to OPM. As a result of these recently completed efforts, the DSS reports accountability for all laptops and hard drives linked to this effort. No further actions are recommended.

While it has been reported that no PII has been associated with an adverse event related to this matter, I recommend DSS establish a process to provide credit monitoring or account restoration services to all persons who demonstrate a credit or identity theft issue associated with this laptop/hard drive transfer matter.

The DoD IG Report included the following recommendation:

"We recommend that the Director of the Defense Privacy Office continue working with the Office of the Assistant Secretary of Defense (Network Information and Integration)/DoD Chief Information Officer (NII/CIO) and the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD AT&L) to develop overarching guidance on the protection of PII on mobile computing devices and give an estimated completion date."

Revised

Do Not Concur:

The DoD IG Audit recommends that the Defense Privacy Office develop a single overarching policy memorandum for the protection of PII that combines the provisions of the:

- DoD CIO Memorandum Department of Defense Guidance on Protecting Personally Identifiable Information (PII)" dated August 18, 2006
  DoD CIO Policy Memorandum "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media," dated July 3, 2007
- Director, Administration and Management Memorandum on "Safeguarding Against and responding to Breaches of Personally Identifiable Information (PII)" dated September 21, 2007.
- USD AT&L issued DoD Instruction 5400.64, "Accountability and Management of DoD-Owned Equipment and other Accountable Property.

I do not concur with the suggestion that the three memoranda mentioned above should be combined into a single AT&L Directive or overarching policy memorandum. Due to the complexity of the issues, the memoranda should remain as separate stand alone documents. To combine the memoranda would not serve the users and would only confuse them. At this time no change is required. However, it is anticipated the memoranda will be incorporated into various DoD regulations and instructions as they are updated.

Collaboration between the Defense Privacy Office and the Office of the Assistant Secretary of Defense NII/DoD CIO is ongoing with the goal of increasing the levels of protections afforded to PII throughout the DoD. Therefore, no specific completion date can be established. Recommend this action be closed.

Michael B. Donley
Senior Agency Official for Privacy

Defense Security Service Comments

DEFENSE SECURITY SERVICE
1340 BRADDOCK PLACE
ALEXANDRIA, VA 22314-1651

MAY 0 2 2008

MEMORANDUM FOR THE DEPARTMENT OF DEFENSE, INSPECTOR GENERAL
(ATTN: KIMBERLY A. CAPRIO)

SUBJECT: Defense Security Service Response to the Draft Department of Defense
Inspector General Report, "Accountability for Defense Security Service
Assets with Personally Identifiable Information"

This memorandum provides the Defense Security Service (DSS) response to the
recommendations and findings identified in the Department of Defense Inspector General
(DoD IG) draft report entitled "Accountability of Defense Security Service Assets with
Personally Identifiable Information." In its report, the DoD IG made ten recommendations.
DSS concurs with **six** of the DoD IG's recommendations and respectfully non-concurs with
four. Additionally, this memorandum provides suggested technical corrections that DSS
previously noted in its response to the discussion draft, but which were not fully incorporated
into the final draft report.

BACKGROUND

In February 2005, while under former management and at the direction of DoD, DSS
transferred the agency's personnel security investigation (PSI) function to the Office of
Personnel Management (OPM), a transition which involved more than 1,500 employees and
numerous pieces of equipment. Pursuant to an agreement between DoD and OPM, OPM
was required to return certain equipment to DSS following the transition. Unfortunately,
during and after the transfer, guidance on what equipment would be returned to DSS and
how that equipment would be returned had changed numerous times. In addition, during the
transfer, the entire DSS property book team had migrated to OPM. Moreover, because the
PSI transition to OPM had been a complete transfer of function, equipment had not
transferred between people, which may have resulted in confusion regarding DoD
accountability requirements for "loaned" equipment. As a result, the agency's controls and
recordkeeping for property accountability during the transition period were weak or
nonexistent.

In July 2006, I requested that the DoD IG conduct an audit to determine whether
DSS had effective internal controls over financial management of its funds. In November
2006, the DoD IG's audit was expanded to include a determination of whether DSS had
adequate controls and accountability of assets containing sensitive personal data or
classified information and whether DSS had properly secured assets in the transition of
the PSI function. DSS received the DoD IG's final draft report on March 4, 2008.
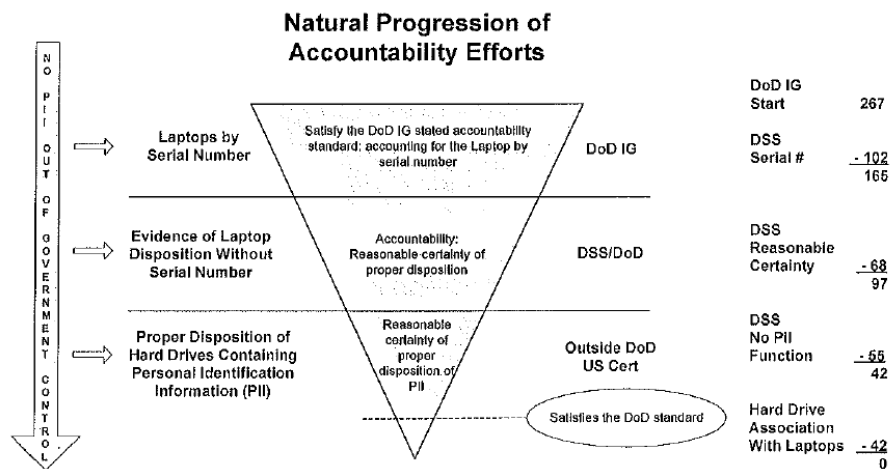
<u>LAPTOP ACCOUNTABILITY</u>

In its report, the DoD IG states that during the course of the audit, DoD IG, DSS, and OPM personnel accounted for 308 of the 501 unaccounted for laptops by "unique identifier," leaving 193 laptops not fully accounted for. DSS believes the DoD IG has mischaracterized the accountability standard of unique identifier, by only considering a laptop fully accounted for through scanned copies of the back of a laptop, a DD Form 1348-1A with serial number, or a DA Form 3161 with serial number. The DoD IG report acknowledges that DSS has obtained information that further accounted for 186 of the remaining 193 laptops, which left only seven unaccounted for laptops as of February 11, 2008. However, based on additional coordination with OPM and the use of a new investigative methodology with regard to laptop turn-in documentation, DSS has accounted for the seven previously unaccounted for laptops.

Prior to receiving the DoD IG's draft report, DSS had accounted for 186 of the 193 laptops using a naturally progressive accountability investigation. The agency first attempted to satisfy the DoD IG standard for property accountability by only accepting scanned copies of the laptop, DD Form 1348-1A, and DA Form 3161 as serial number identification. DSS then accounted for additional laptops by applying a standard of "reasonable certainty." The agency's investigative methodologies included compiling Defense Reutilization Marketing Office (DRMO) and Directorate of Logistics (DOL) turn-in documentation, examining laptop warranty return processes, researching laptop transaction histories in the Defense Property Accountability System (DPAS), and analyzing hard drives. Finally the agency attempted to ensure, to a reasonable degree of certainty, that any personally identifiable information (PII) that the unaccounted for laptops may have contained was properly disposed of or safeguarded.

DSS analyzed the hard drives and the hard drive disposal process as part of the accountability investigation because fully accounting for all laptops would not necessarily account for all PII, since PII would reside on a laptop's hard drive, a removable component. During its audit, the DoD IG conducted a sample of 33 hard drives and determined that 17 contained PII. **(Many of these hard drives contained PII of the DSS agent to whom the hard drives were assigned and not PII related to the subjects of security clearance investigations.)** To ensure proper controls, DSS examined its hard drive storage, reformatting, and disposal processes. After completing the hard drive analysis, DSS confirmed that it has continued to dispose of hard drives in accordance with National Security Agency guidance for disposition of classified information. DSS determined, with reasonable certainty that any PII associated with previously unaccounted for laptops had been accounted for after receiving certification statements from DSS and OPM employees who process hard drives for destruction. These certifications account for a total of 5,665 laptop hard drives that have been properly handled or disposed of by DSS and OPM.

2

After receiving the DoD IG's draft report, DSS reexamined all DRMO and DOL turn-in documents for laptops identified by serial number. The agency had not previously compared these serial numbers to DPAS records to ensure that turned in laptops had not been erroneously labeled due to an operator entry error. Any turn-in document that contained a laptop serial number that did not appear in DPAS meant that the laptop had been misidentified on that document. DSS discovered that DRMO and DOL turn-in documents for seven of the laptops contained erroneous serial numbers. DSS then compared these erroneous serial numbers to the serial numbers of the remaining unaccounted-for laptops. DSS identified seven of the previously unaccounted-for laptops with serial numbers differing by just one digit from the serial numbers written on the turn-in documents. The serial numbers on the turn-in documents are not on any property book or any other accounting documents. These anomalies may be attributed to typographical errors which have since been corrected. Thus, DSS has now accounted for all of the previously unaccounted for laptops through its naturally progressive investigation.

Revised

Natural Progression of Accountability Efforts

	DoD IG Start	267
Laptops by Serial Number — Satisfy the DoD IG stated accountability standard: accounting for the Laptop by serial number (DoD IG)	DSS Serial #	-102
		165
Evidence of Laptop Disposition Without Serial Number — Accountability: Reasonable certainty of proper disposition (DSS/DoD)	DSS Reasonable Certainty	-68
		97
Proper Disposition of Hard Drives Containing Personal Identification Information (PII) — Reasonable certainty of proper disposition of PII (Outside DoD US Cert)	DSS No PII Function	-55
		42
Satisfies the DoD standard	Hard Drive Association With Laptops	-42
		0

(Left vertical axis: NO PII OUT OF GOVERNMENT CONTROL)

This accounting for the final seven laptops supports the additional risk-mitigating factors that the agency's investigation revealed. For example, neither the DoD IG's audit nor the DSS investigation uncovered any evidence of theft or malicious intent. Indeed, in the nearly four years since the PSI function transfer, there has not been a single report of loss or compromise of the DSS laptops or any PII contained on the laptop hard drives. Moreover, DSS reemphasizes that it maintains signed certifications indicating that the agency properly stored or disposed of more than 5,600 hard drives in accordance with DoD guidelines. The agency also has records demonstrating that it properly disposed of more than 1,800 laptops.

3

In accordance with the reporting requirements of DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007, and the Director of Administration and Management Memorandum (DA&M), "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," September 21, 2007, DSS in January 2008 determined that public notification of potential compromise of PII was not warranted, and briefed the Defense Privacy Office (DPO). The September 21, 2007 DA&M memorandum implements the test established in the Office of Management and Budget (OMB) Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007. The September 21, 2007 DA&M memorandum requires that DoD Components conduct a two-part test when determining whether public notification of a PII breach is required.

Under the DA&M memorandum's two-part test, DoD Components must assess (1) the "likely risk of harm" and (2) the "relative likelihood of the risk occurring." When assessing the "likely risk of harm," DoD Components are instructed to consider five factors: (1) the nature of the data elements breached, (2) the number of individuals affected, (3) the likelihood the information is accessible and usable, (4) the likelihood the breach may lead to harm, and (5) the ability of the agency to mitigate the risk of harm. (See page 10 and Appendix A of the September 21, 2007 DA&M memorandum). The DA&M memorandum provides a "DoD Privacy Risk Level Table" to assist DoD Components in assessing the "likelihood of the risk occurring" (or "risk level"). (See page 10 and Table 1, "Risk Assessment Model," of the September 21, 2007 DA&M memorandum). After considering the factors outlined in Appendix A and Table 1 of the September 21, 2007 DA&M memorandum, the agency determined that there was little or no likelihood that a breach of PII had occurred. In making that determination, DSS considered the fact that there was no evidence that any laptops or hard drives were stolen or ever outside of government control. Moreover, through its ongoing search efforts, DSS was continuing to locate unaccounted for laptops and hard drives and the agency believed that it would ultimately be able to account for all of the remaining laptops and hard drives. Because the risk of harm and the likelihood of the risk occurring were low, DSS determined that public notification of a potential breach would create unnecessary concern and confusion among those individuals who may be affected by the potential breach. Therefore, in accordance with OMB and DoD guidance, the agency concluded that public notification was not required. Having accounted for all of the previously unaccounted for laptops, due to the additional efforts since the publication of the DoD IG draft report, DSS maintains its conclusion.

DSS senior leadership informed DPO of its determination in a memorandum dated January 15, 2008. As noted above, after receiving the DoD IG's draft report, DSS was able to account for all of the remaining unaccounted for laptops. Accordingly, on May 2, 2008, the agency provided an amended copy of the January 15 memorandum to DPO (see next page). Significantly, DPO agreed with the agency's determination that public notification was not warranted.

4

MEMORANDUM FOR DIRECTOR OF ADMINISTRATION AND MANAGEMENT

SUBJECT: Determination Regarding Public Notification of Potential PII Breach -
               Corrected Copy (May 2, 2008)

      This memorandum recounts background information regarding the subject stated
above, and states my determination regarding this subject.

<u>Background</u>

      In July 2006, I requested that the Department of Defense Inspector General (DoD
IG) conduct an audit to determine whether DSS had effective controls over financial
management of its funds. In November 2006, the DoD IG's audit was expanded to
include a determination whether the Defense Security Service (DSS) had properly
accounted for laptop computers that were used by DSS personnel security investigators
who transferred to the Office of Personnel Management (OPM) in February 2005.

      As a result of the DoD IG's preliminary findings, on August 10, 2007, I directed
that a DSS special investigative team determine the disposition and whereabouts of 267
laptops that the DoD IG team identified as unaccounted for. In conducting its
investigation, the DSS team focused primarily on the disposition, safeguarding, and
potential compromise of Personally Identifiable Information (PII) that the unaccounted
for laptop hard drives may have contained.

      The DSS team's investigation consisted of four phases:

- A detailed search of all DSS office spaces, vehicles, desks, cabinets and
  other containers;
- A thorough analysis of turn-in documents maintained by the Defense
  Reutilization and Marketing Office (DRMO) and the Directorate of
  Logistics (DOL), laptop warranty return processes, laptop transaction
  histories in the Defense Property Accountability System (DPAS), and
  hard drive user profiles; and
- An analysis of the agency's hard drive handling and disposal process to
  determine the potential breach of PII.

      During its investigation the agency located 81 previously unaccounted for laptops
through physical searches and serial numbers on DRMO and DOL documents, and
accounted for an additional 21 laptops by serial number through DPAS transaction

<div align="center">5</div>

history records. DSS was also able to account for 68 laptops through DRMO turn-in documents and warranty replacements, 55 laptops due to their lack of association with any DSS function that involved the use or storage of PII, and 42 laptops through hard drive analysis. Furthermore, DSS and OPM certified that more than 5,600 hard drives were properly accounted for in accordance with the National Security Agency (NSA) "Storage Device Declassification Manual."

The above efforts enabled DSS to account for, with reasonable certainty, all of the 267 laptops that the DoD IG had identified as unaccounted for.

DSS Determination Regarding Public Notification

In accordance with the reporting requirements of DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007, and the Director of Administration and Management Memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," September 21, 2007, I am hereby advising you that, as Director of the Defense Security Service (DSS), I have determined that public notification of the potential compromise of PII is not warranted.

Applying the risk assessment factors outlined in Appendix A and Table 1 of the Director of Administration and Management's September 2007 memorandum, I find that there is little or no likelihood that a breach of PII has occurred. In support of this conclusion, I note that there is no evidence that the DSS laptops or any PII contained on the laptop hard .drives were stolen or ever outside of government control. I also find that the certification of proper storage and destruction of more than 5,600 hard drives, the component that would contain PII, is reliable evidence of no loss or compromise of PII, Furthermore, because the risk of harm is low, I believe that public notification would create unnecessary concern and confusion among those individuals who may be affected by the potential breach. Accordingly, for the foregoing reasons, I have determined that public notification is not required.

//original signed//
Kathleen M. Watson
Director

Attachment:
Briefing to DoD Privacy Office, May 2, 2008

6

While DSS has accounted for all of the previously unaccounted for laptops, the agency is continuing its effort to locate all equipment disposition records. During the course of the DSS investigation, DRMO provided significant assistance. However, due to its records disposition cut-off date policy and move to document automation, DRMO was unable to provide DSS with all of the requested turn-in documents. As a result, DSS and DoD IG are continuing to conduct a joint effort to obtain DSS equipment turn-in records from other sources.

COMMON ACCESS CARD / SECURITY CONTAINER ACCOUNTABILITY

In July 2006, the DSS Security Office began the process of reconciling DoD civilian Common Access Cards (CACs) still in the possession of DSS personnel who transferred to OPM. DSS has since accounted for all of the DoD civilian CACs that were issued under the auspices of DSS to personnel who subsequently transferred to OPM.

An additional seven DoD CACs were researched during this process and determined to have been issued to OPM employees after the transfer. DSS did not issue these seven CACs, had no involvement in their issuance, and was not responsible for their retrieval. It should be noted that OPM is in the process of reconciling these seven CACs, and only one of them remains unaccounted for. There are no outstanding CAC issues relating to the DSS/OPM transfer. Documentation providing closure to this initiative was sent to the DoD IG via DSS memorandum dated February 20, 2008.

DSS has obtained a final accounting of the safes transferred to OPM, based on the available data within DPAS and OPM records. DSS worked extensively with OPM to identify the transferred safes and their contents. At the request of the DSS Security Office, OPM identified in writing that DSS transferred 23 safes to OPM, and further certified that none of these safes contained sensitive or classified material. All 23 safes were fully accounted for by DSS and certified against OPM records and DPAS. Since the DoD IG audit, DSS has implemented enhanced internal control measures for safe accountability within the agency.

The DoD IG draft report does not fully address the agency's risk management assessment regarding the safes transferred to OPM. DSS determined that no additional action regarding safe accountability was warranted since (1) at the request of DSS, OPM conducted a thorough search and documented receipt of all known DSS safes, (2) the safes were transferred to OPM "in-place," i.e., they were not shipped, but transferred with the physical location that transferred to OPM, which significantly reduced the probability of them being lost or misplaced, and (3) OPM certified that none of the 23 safes transferred to OPM contained sensitive or classified material. DSS has obtained a final accounting of the safes transferred to OPM, based on all available data and resources. This information was previously provided to the DoD IG on February 11, 2008.

7

<u>ASSET ACCOUNTABILITY</u>

Throughout its report, the DoD IG references DoD Instruction 5000.64, "Accountability and Management of DoD-Owned Equipment and Other Accountable Property," in support of its contention that all property containing sensitive information must be tracked by serial number or other unique identifier. By requiring serial number accountability, the DoD IG is holding DSS to a higher standard than what is currently mandated by DoD. DoD Instruction 5000.64 establishes policy and procedures for the accounting of DoD-owned property. Paragraph 6.2.1. of that instruction provides that "[a]ccountable property records shall be established for all property purchased, or otherwise obtained, having a unit acquisition cost of $5,000 or more; leased assets (capital assets) of any value; and assets that are sensitive or classified (see Volume 10, Table 61 of DoD 4100.39-M (Reference (k)).["](1) The definition of "sensitive information" contained in the DoD IG draft report is inconsistent with the term "sensitive items" as used and defined in DoD Instruction 5000.64.

In defining sensitive and classified assets, subparagraph 6.2.1 of DoD Instruction 5000.64 (subparagraph 5.3.1. of the 2002 version) cites Volume 10, Table 61 of DoD Manual 4100.39. Significantly, the list of "sensitive items" in Table 61 does not include laptops, hard drives, or other Information Technology (IT) equipment containing PII. Instead, Table 61 includes "sensitive" items such as nonnuclear missiles and rockets; arms, ammunition and explosives; drugs and other controlled substances; and precious metals. Moreover, in subparagraph E2.16.2 of DoD Instruction 5000.64, "sensitive items" is defined as: "Property requiring a high degree of protection and control due to statutory requirements or regulations (e.g., narcotics and drugs, precious metals, high value or highly technical assets, hazardous assets, or small arms, ammunition, explosives, and demolition material).["](2) Nowhere in DoD Instruction 5000.64 (the current or 2002 versions) does it state that DoD Components must track IT equipment or other items containing PII by serial number or other unique identifier. DoD Instruction 5000.64 provides policy and procedures for DoD property accountability and does not prescribe

---

[1] Since the current November 2, 2006 version of DoD Instruction 5000.64 did not exist during the period of the DSS/OPM PSI transition (August 2004 – February 2005), the August 13, 2002 version of the instruction would be applicable to this matter. Nonetheless, paragraph 5.3.1 of the 2002 version of DoD Instruction 5000.64 contains nearly identical language to paragraph 6.2.1 of the current instruction. Paragraph 5.3.1 of the 2002 version provides, in relevant part, that "[a]ccountable property records shall be established for all property purchased, leased (capital leases), or otherwise obtained, having a unit acquisition cost of $5,000 or more . . ., and items that are sensitive or classified. (See Volume 10, Table 61 of DoD 4100.39-M (reference (j)).)" See DoD Instruction 5000.64, "Defense Property Accountability," August 13, 2002. Likewise, the language found in the previous version of Volume 10, Table 61 of DoD 4100.39-M is nearly identical to that found in the current version (updated October 2007) and does not include laptop computers in its lists of sensitive or classified items.

[2] The definition of "sensitive items" found in the 2002 version of DoD Instruction 5000.64 is nearly identical to the definition found in the current version. Subparagraph E2.1.12.2 of the 2002 version defines "sensitive items" as: "Items that require a high degree of protection and control due to statutory requirements or regulations, such as narcotics and drug abuse items; precious metals; items that are of a high value, highly technical, or a hazardous nature; and small arms, ammunition, explosives, and demolition material."

8

PII accountability or safeguarding guidelines. In addition, the DoD IG's conclusion that all laptops should be tracked using a unique identifier presumes that all laptops contain PII. Clearly, not all laptops within DoD contain PII. In fact, in the present case, the forensic analysis conducted by the Defense Criminal Investigative Service (DCIS) in November 2006 revealed that only a little more than half of a sample of recovered DSS hard drives tested contained PII.

The DoD IG report addresses planning and maintaining accountability for DSS assets. During the course of the DoD IG audit, DSS has continuously worked to improve property accountability by analyzing shortcomings within the process and making corrections. DSS has identified, documented, and is implementing new processes to ensure accountability of all Property, Plant and Equipment (PP&E) across the agency by clearly defining accountable property, to address regular inventories, and to maintain accountability for all DSS assets. DSS has modified the processes for procurement, receipt, and accountability of incoming assets to ensure that all property received is increased in DPAS prior to being issued. The DSS Support Services Office and the DSS Office of the Chief Information Officer (CIO) are refining processes and taking steps required to capture accountable IT property in DPAS. This will allow full visibility across the enterprise and allow real-time updates to DPAS.

The CIO conducted a 100% inventory of IT assets within DSS between March and December of 2007. Effective March 31, 2008, the DSS Support Services Office has detailed one full-time employee to the CIO to integrate the results of that inventory into DPAS, and also to provide DPAS training and guidance to the CIO on management of the assets. The DSS Support Services Office conducted an inventory of accountable property at DSS headquarters between May and October 2007. Barcodes were assigned to all accountable assets located at DSS headquarters, including safes. As safes without barcodes were identified at field locations, DPAS was updated and barcodes were issued. DSS coordinated with OPM and properly turned the remaining assets in to the DRMO.

The DSS Support Services Office recently updated the agency's property management regulation (DSS Regulation 15-2, "Property Management"), which became effective on February 8, 2008. The updated regulation establishes agency accountability and management policy and responsibilities, as well as reduces the span of control for assets to the lowest level of accountability. The DSS Support Services Office's property management staff has been increased to include a GS-13 team leader and five support contractors including the detailed full-time employee for the CIO. The implementing guidance for DSS Regulation 15-2, in the form of an operating instruction (OI), is currently under development with a planned publication in the third quarter of this fiscal year. The OI will define accountable and pilferable assets in accordance with DoD guidance and address in detail the procedures for the procurement, receipt, transfer, inventory and disposal of DSS assets.

9

The DSS Support Services Office is currently seeking a vendor and contracting vehicle to conduct a 100% physical wall-to-wall inventory of DSS PP&E to facilitate the transfer of the property book to the new Property Book Officer (PBO). DSS expects to complete the inventory, reconciliation, and transfer of the property book by the first quarter of fiscal year 2009.

AGENCY RESPONSE TO REPORT RECOMMENDATIONS

Overall, the DoD IG report identified 10 recommendations. DSS respectfully concurs with six of the DoD IG's recommendations and respectfully non-concurs with four. The DoD IG's individual recommendations and the agency's respective responses are set forth below:

Recommendation 1(a): Maintain an audit trail showing all transactions from acquisition to disposal for assets that contain sensitive or classified information in accordance with DoD Instruction 5000.64, "Accountability and Management of DoD-Owned Equipment and Other Accountable Property," November 2, 2006.

DSS Response: Concur

The DSS Property Management Regulation became effective on February 8, 2008 and assigns responsibilities at all levels for the management and accountability of DSS assets throughout each asset's life cycle. Effective March 31, 2008, the DSS Support Services Office has detailed one full-time employee to the CIO to assist in the integration of property information currently maintained on electronic spreadsheets into DPAS, and to provide guidance and support to the CIO for the life cycle management and accountability of IT assets.

In addition, DSS is developing property management operating instructions that further define processes and procedures for the accountability and management of DSS PP&E, with an anticipated publication of the early third quarter of fiscal year 2008.

Recommendation 1(b): Conduct periodic physical inventory of laptops and other assets that contain personally identifiable information.

DSS Response: Concur

The DSS property management regulation requires that a 100% physical inventory of all DSS PP&E be conducted and reconciled annually. The operating instruction provides guidance on the inventory process. Random spot inventories, individual hand receipt inventories, etc., will be conducted regularly in addition to the annual inventory to ensure that all property is being managed and maintained properly. A 100% physical inventory of all DSS assets is planned. DSS is currently seeking a vendor to provide a service and a

10

contracting vehicle to use to acquire the service. Anticipated start in the third quarter of fiscal year 2008 with reconciliation completed, certification and transfer of Property Book to new PBO by the first quarter of fiscal year 2009.

Recommendation 1(c): Track assets that contain personally identifiable information using a unique identifier, such as a serial number or barcode.

DSS Response: Concur

Because PII could be stored on any IT device capable of storage to include Blackberries, laptops desktops, printers, etc., DSS did not segregate laptops or other IT equipment for special consideration, given the scheduled and random inventories throughout the year. All assets that could contain PII shall be tracked by serial number and barcode in DPAS throughout there life cycle.

Recommendation 1(d): Report any future confirmed or unconfirmed instances of unauthorized disclosure of personally identifiable information to US-CERT and the Defense Privacy Office in accordance with Office of Management and Budget memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology investments," July 12, 2006, and with DoD Directive 5400.11-R, "DoD Privacy Program," May 14, 2007.

DSS Response: Concur

DSS will continue to comply, as it has in the past, with DoD and OMB reporting requirements for potential breach or compromise of PII.

Recommendation 1(e): Establish guidelines and training that DSS employees must follow to protect PII from unauthorized disclosure.

DSS Response: Concur

DSS will create PII protection training and make it part of the DSS New Employee Orientation Program, as well as add it as an annual training requirement for the DSS work force. DSS will have the first iteration ready by June 30, 2008.

Recommendation 1(f): The DoD IG recommends that DSS continue to coordinate with OPM to account for remaining unaccounted for laptops.

DSS Response: Non- concur

11

51

DSS has maintained a continual dialogue with OPM throughout its laptop accountability investigation. Corresponding personnel from DSS and OPM met to discuss and develop laptop accountability methodology on September, 21, 2007, October 23, 2007, November 15, 2007, and December 12, 2007. Email and telephonic communication between the two agencies occurred several times weekly since August 2007. DSS also retrieved hard drives from OPM on December 12, 2007 and February 7, 2008. DSS and OPM agreed to maintain open dialogue and continue coordination, as necessary, to account for the final seven laptops.

DSS personnel met with OPM personnel on April 8, 2008 in an effort to obtain additional information on a potential lead that could have accounted for the final seven laptops. However, DSS has since accounted for the remaining seven laptops through a review of DSS turn-in documents. Therefore, there is no longer a need for DSS to continue its coordination efforts with OPM.

Deleted

Recommendation 1(g): After exhausting all possibilities for locating the unaccounted for laptops, plan and implement steps to mitigate the risk of unauthorized disclosure of the personally identifiable information stored in those laptops.

DSS Response: Non-concur

As noted above, DSS has accounted for the remaining seven laptops. Thus, there is no longer a need for the agency to plan and implement risk mitigation.

Deleted

Recommendation 1(h): The DoD IG recommends that DSS continue efforts to locate the remaining seven unaccounted for Common Access Cards.

DSS Response: Non-concur

DSS has accounted for all of the DoD civilian CACs that were issued under the auspices of DSS to personnel who subsequently transferred to OPM. An additional seven DoD CACs were researched during this process and determined to have been issued to OPM employees after the transfer. DSS did not issue these seven CACs, had no involvement in their issuance, and was not responsible for their retrieval. There are no outstanding CAC issues relating to the DSS/OPM transfer. Documentation providing closure to this initiative was sent to the DoD IG via DSS memorandum dated February 20, 2008.

Deleted

Recommendation 1(i): The DoD IG recommends that DSS obtain a final accounting of safes that DSS transferred to OPM.

DSS Response: Non-concur

12

DSS has obtained a final accounting of the safes transferred to OPM, based on the available data within DPAS and OPM records. DSS worked extensively with OPM to identify the transferred safes and their contents. At the request of the DSS Security Office, OPM identified in writing that DSS transferred 23 safes to OPM, and further certified that none of these safes contained sensitive or classified material. All 23 safes were fully accounted for by DSS and certified against OPM records and DPAS. Since the DoD IG audit, DSS has implemented enhanced internal control measures for safe accountability within the agency.

DSS determined that no additional action regarding safe accountability was warranted since (1) at the request of DSS, OPM conducted a thorough search and documented receipt of all known DSS safes, (2) the safes were transferred to OPM "in-place," i.e., they were not shipped, but transferred with the physical location that transferred to OPM, which significantly reduced the probability of them being lost or misplaced, and (3) OPM certified that none of the 23 safes transferred to OPM contained sensitive or classified material. DSS has obtained a final accounting of the safes transferred to OPM, based on all available data and resources. DSS provided this information to the DoD IG on February 11, 2008.

Recommendation 1(j): Issue guidance that requires DSS to perform a physical inventory every year in compliance with DoD Instruction 5000.64.

DSS Response: Concur

DSS Regulation 15-2, "Property Management," which became effective on February 8, 2008, provides this guidance and will be supplemented with more specific processes and procedures in the near future.

TECHNICAL CORRECTIONS

Below are the agency's responses to several statements contained in the draft DoD IG report which it believes to be factually inaccurate. DSS respectfully requests that the following corrections be made to the final report prior to its issuance.

➢ Page 2, first paragraph, last sentence. The title of the transition team member mentioned as the "Under Secretary of Defense for Counter Intelligence and Security" should be "Deputy Under Secretary of Defense for Counterintelligence and Security."

➢ Page 7, last footnote. The position of Chief of Support Services is currently filled. The footnote should state that the Chief of Support Services referenced in this report has retired from DSS. It is preferred that all references to the Chief of DSS Support Services state "former," rather than using the footnote as there is one

13

place in the report where "former" was placed before the Chief of DSS Support Services.

➤ Page 7 continuing to page 8, last paragraph, second sentence. The inventory records analyzed to determine that DSS transferred 249 of the 501 laptops to OPM were DPAS records. The numbers were retrieved from a DPAS report that was exported to a Microsoft Excel document as an inventory list of assets transferred to OPM.

Revised
second
bullet

➤ Page 9, fourth bullet. DSS and the DoD IG were still reviewing DRMO forms through November 2007. DA 3161 forms were also reviewed for transactions processed out of agency to the Directorate of Logistics (DOL).

third bullet

➤ Page 9, fifth and sixth bullet. The interviews of former and current DSS and OPM employees listed in DPAS as the last to have custody of the unaccounted for laptops were conducted between December 2006 and July 2007. These interviews were only for two models of IBM laptops and did not include the additional 13 laptop models in use by DSS during the period of time the covered by the audit.

Revised

➤ Page 10, second paragraph, second bullet. The list of 501 laptops originally unaccounted for came from DPAS records. The assets sent to the DRMO without identifying information were not removed from the DPAS system under that document number or on that day. DSS has determined with a reasonable degree of certainty that the 65 laptops accounted for in this manner **are** part of the 193 "unaccounted for" laptops.

Revised

➤ Page 13, last paragraph, last sentence. The DSS Security Office began the process of reconciling the CACs in July 2006, when it became evident within the agency that the DSS Transition Team had not retrieved the CACs issued to DSS personnel who transferred to OPM, as recommended to the team by the DSS Security Officer. The current DoD IG draft report does not clearly indicate that DSS began reconciling the CACs in July 2006; it infers that no action was taken until February 2007. DSS first contacted Defense Manpower Data Center (DMDC) for assistance in August 2006, not February 2007, as inferred in the draft DoD IG report. Efforts to identify and retrieve the CACs were not completed until February 20, 2008, due to the lack of DSS Transition Team records and extensive coordination with DMDC. DSS provided documentation regarding these efforts to the DoD IG throughout the process.

Revised

➤ Page 15, last paragraph, first sentence. Sentence states that hundreds of CACs, safes, laptops, and auxiliary hard drives were transferred to OPM on an informal, verbal agreement. "Hundreds" should be changed to "a significant number," as

14

54

the sentence could otherwise be misconstrued to mean that hundreds of each type of these items were transferred.

> Page 17, third paragraph, first sentence. Improsive **removed** disposed of laptops **from** DPAS not entered disposed of laptops in DPAS. MZM did not ship all laptops directly to DRMO, this only happened occasionally.

> Page 24, third paragraph, first sentence. One of the employees interviewed is listed as the "former DSS Assistant to the Director." The correct title for this person is the former Assistant to the former DSS Acting Director.

> Page 27, second paragraph, first, second and third sentences. The DoD IG states that DSS accurately recorded only two of the seven laptop computers of the 50 DPAS records analyzed. This statement specifically relates to IBM laptops and not all laptops within DSS. After the review of DoD IG documentation regarding the 2 of 7, the above statement was determined by **both DSS and the DoD IG** to be incorrect. **A detailed analysis of the 7 IBM laptops showed 5 were accurate and 2 were not.** As seen in the referenced two sentences, they contradict each other.

DSS appreciates the opportunity to respond to the findings and recommendations made in the DoD IG's draft report. To the extent that DSS has failed to comply with DoD guidelines or procedures, current management is committed to improving its operations to ensure that these guidelines and procedures are followed in the future. Indeed, as stated above, DSS has already taken steps to ensure the proper accountability and management of Government-owned property and the safeguarding of assets containing PII.

If you have any questions or require and additional information, please do not hesitate to contact me or Mr. Douglas Stone, DSS Inspector General, at (703) 325-5318 or douglas.stone@dss.mil.

Kathleen M. Watson
Director

15

Team Members

The Department of Defense Office of the Deputy Inspector General for Auditing, Readiness and Operations Support prepared this report. Personnel of the Department of Defense Office of Inspector General who contributed to the report are listed below.

Paul J. Granetto
Robert F. Prinzbach II
Kimberley A. Caprio
Patricia A. Papas
Rhonda L. Ragsdale
Robert P. Goldberg
Andrew R. MacAttram
David A. Palmer
Antwan Jackson
Bridgette A. Seebacher
Marlene Cruz-Freire

Inspector General
Department *of* Defense